arXiv:math/0403181v1 [math.RA] 10 Mar 2004

HAMILTONIAN SELFDISTRIBUTIVE QUASIGROUPS

Dolors Herbera, Tomáš Kepka, and Petr Němec

Abstract. The problem of the existence of non-medial distributive hamiltonian quasigroups is solved. Translating this problem first to commutative Moufang loops with operators, then to ternary algebras and, finally, to cocyclic modules over $\mathbb{Z}[x, x^{-1}, (1-x)^{-1}]$, it is shown that every non-medial distributive hamiltonian quasigroup has at least 729 elements and that there are just two isomorphism classes of such quasigroups of the least cardinality. The quasigroups representing these two classes are anti-isomorphic.

0. Introduction

The first explicit allusion to the left and right instances of selfdistributivity (i.e., $(x(yz) \doteq (xy)(xz)$ and $(xy)z \doteq (xz)(yz))$ seems to appear in [39] where one can read the following comment: *"These are other cases of the distributive principle. ... These formulae, which have hitherto escaped notice, are not without interest."* Another early work [43] already contains a particular example of a (self)distributive quasigroup:

	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

This quasigroup is necessarily non-associative and plays a principal rôle in the structure theory of distributive (or, more generally, trimedial) quasigroups (see e.g. [2], [3], [5], [6], [19], [35] and [48]).

The first article fully devoted to selfdistributivity is (perhaps) [11] (see also [49] and [32]) where, among others, normal subquasigroups are studied and an attempt is made to show that every minimal subquasigroup of a (finite) distributive quasigroup is normal (see also [15]). Actually, the latter assertion is not true. All non-medial symmetric distributive quasigroups (alias non-desarguesian planarily affine triple systems) serve as counterexamples and first constructions of these can

1991 *Mathematics Subject Classification.* 20N05.

Key words and phrases. Quasigroup, distributive, medial, hamiltonian.

The research of the first author was partially supported by the DGI and the European Regional Development Fund, jointly, through Project BFM2002-01390, and by the Comissionat per Universitats i Recerca of the Generalitat de Catalunya. The second author was supported by the institutional grant MSM 113200007 and by the Grant Agency of Charles University, grant #269/2001/B-MAT/MFF, the third author by the Grant Agency of Czech Republic, grant #GAČR-201/02/0594.

be found in [9] and [17]. However, the paper [11] may be regarded as the starting point for the investigation of normality problems in distributive quasigroups.

Hamiltonian groups (i.e., (non-commutative) groups having only normal subgroups) were described (and named after W. R. Hamilton) by R. Dedekind in [13] and it was shown in [38] that a similar description takes place for hamiltonian Moufang loops, too. Furthermore, all subquasigroups of medial quasigroups (i.e., quasigroups satisfying the identity $(xy)(uv) \doteq (xu)(yv)$) are normal. That is, these quasigroups are hamiltonian. (Notice that abelian groups are included in hamiltonian structures in this paper – not usual, but technically advantageous.)

A thorough treatment (remarkable also for epic width) on cancellative distributive groupoids was written by J.-P. Soublin ([48]). Section IV.9 of [48] is devoted to normal subquasigroups of distributive quasigroups and, among others, it is shown that every hamiltonian symmetric (i.e., satisfying the identities $xy \doteq yx$ and $x(xy) \doteq y$) distributive quasigroup is medial. Moreover, an open problem whether there exist non-medial hamiltonian distributive quasigroups is formulated ([48], p. 175). The main aim of the present paper is to solve this problem.

In [42], it is claimed that every hamiltonian quasigroup which is either distributive or a CH-quasigroup (i.e., a symmetric quasigroup satisfying the identity $(xx)(yz) \doteq (xy)(xz)$), is medial. The proof is based on the idea that if H is a subloop of a commutative Moufang loop G and the subloop generated by H and the centre of G is normal then H is normal. However, this assertion is false, any non-associative commutative Moufang loop nilpotent of class 2 serving as an easy counterexample (in this case, every subloop containing the centre is normal and G contains a non-normal subloop). Moreover, 3.2 and 8.9 are examples of non-medial hamiltonian distributive or CH-quasigroups, respectively.

A possible way how to construct non-medial hamiltonian distributive quasigroups is suggested in [22], but the paper is almost unreadable and much more has to be done. However, the basic idea is working, and the problem is transferred, step by step, first to commutative Moufang loops with operators, then to certain ternary algebras and, finally, to some cocyclic modules. Actually, the problem of finding non-medial hamiltonian distributive quasigroups is equivalent to the construction of (finite) cocyclic modules over the ring $\mathbb{Z}[x, x^{-1}, (1-x)^{-1}]$ that cannot be generated by less than three elements. We recall that a cocyclic module is contained in the injective hull of its simple essential socle, so a good understanding of the injective hull of simple modules and its submodules is necessary to solve the problem.

After [37], [30] and [16], if R is a commutative noetherian ring then the structure of some of the indecomposable injective modules over $R[x]$, and hence over a localization of $R[x]$, can be described in terms of modules of divided powers over the indecomposable injectives of R. This is the case for the injective hull of the simple modules over the ring $R[x] = \mathbb{Z}[x]$. Since the indecomposable injective modules over $\mathbb{Z}$ are also well known, a detailed study of the modules of divided powers and some of their finite submodules gives us the desired examples of cocyclic modules, which, after the proper translation, allows us to construct our examples of non-medial hamiltonian distributive quasigroups in a completely explicit way.

Modules of divided powers, also called Macaulay modules, were first known in [33] and, as mentioned before, they are important in connection to the description of injective modules. If K is any field and $K(x)$ is the field of fractions of $K[x]$ then $M = K(x)/K[x]_{(x)}$ is an indecomposable injective module with simple essential socle K. Note that M has $\{x^{-n} + K[x]_{(x)}\}_{n\in\mathbb{N}}$ as K-basis. The modules of divided

powers can be seen as an abstraction of the structure of M to the general setting of modules over a polynomial ring.

The following text is divided into Sections 1 – 12. Basic notions are introduced in Section 1. Section 2 is devoted to normal subquasigroups and Section 3 contains two examples, the second one being (in view of 12.8) the solution of our problem (it could be interesting to show the required properties of this example directly, probably using a computer). In Sections 4 and 5, some basic properties of commutative Moufang loops and quasimodules (i.e., commutative Moufang loops with operators) are investigated. Section 6 deals with ternary representations of quasimodules. Section 7 is devoted to the connection between hamiltonian quasimodules and certain cocyclic modules. In Sections 8 and 9, (hamiltonian) trimedial and distributive quasigroups, respectively, are studied and a transfer to quasimodules is presented. Sections 10 and 11 are devoted to modules of divided powers. In Section 12, a synthesis of the preceding parts is made. The initial problem is solved, but a complete description of non-medial hamiltonian distributive quasigroups is far from being finished.

1. Preliminaries

1.1 (Quasigroups) A non-empty set Q equipped with a binary operation is said to be a *quasigroup* if for all $a, b \in Q$ there exist uniquely determined $x, y \in Q$ such that $ax = b = ya$. A quasigroup with a neutral element (a unit) is a *loop*.

A quasigroup Q is called

- *medial* if $(ax)(yb) = (ay)(xb)$ for all $a, b, x, y \in Q$;
- *trimedial* if every subquasigroup of Q generated by at most three elements is medial;
- *left (right) distributive* if $x(ab) = (xa)(xb)$ ($(ab)x = (ax)(bx)$) for all $a, b, x \in Q$;
- *distributive* if Q is both left and right distributive;
- *symmetric* if $ax = xa$ and $x(xa) = a$ for all $a, x \in Q$;
- a *CH–quasigroup* if Q is symmetric and $(xx)(ab) = (xa)(xb)$ for all $a, b, x \in Q$.

Every distributive quasigroup is idempotent and trimedial ([2]). Every CH–quasigroup is trimedial ([35]). A reader is referred to [2], [3], [11], [12], [15], [18], [35], [40], [48], [49] for many useful prerequisites concerning (distributive, medial, etc.) quasigroups.

1.2 (Commutative Moufang loops) Let Q be a loop satisfying the equation $(xx)(ab) = (xa)(xb)$. Substituting $a = 1_Q$, we get $(xx)b = x(xb)$ and, setting $b = 1_Q$, we get $(xx)a = (xa)x$. Now, if $a = b$, then $x(xa) = (xa)x$ and it follows easily that Q is commutative. Such a loop Q is called a *commutative Moufang loop*. All the details concerning commutative Moufang loops needed in the sequel may be found in [10].

1.3 (Rings and modules) In what follows, $\mathbf{R}$ stands for a (non–trivial) commutative and associative noetherian ring with unit and modules are unitary $\mathbf{R}$–modules with scalars written on the left. Furthermore, we assume that there exists a (ring) homomorphism $\mathbf{\Phi}$ of $\mathbf{R}$ onto the three–element field $\mathbb{Z}_3 = \{0, 1, 2\}$ of integers modulo 3 and we put $\mathbf{I} = \mathrm{Ker}(\mathbf{\Phi})$. Clearly, $\mathbf{I}$ is a maximal ideal of $\mathbf{R}$ and the simple

(three-element) factormodule $_{\mathbf{R}}\mathbf{R}/\mathbf{I}$ will be denoted by $\mathbf{P}$. As concerns various further pieces of information on general rings and modules, a reader is referred to [1], [8] and [50] and to [36] for more specific information on the commutative noetherian setting. A very nice reference for injective modules is the book [44]. The injective modules we study are, in fact, artinian; for some of the results on artinian modules over commutative ring we need the reference [14].

1.4 (Quasimodules) By a *quasimodule* we mean a commutative Moufang loop $Q(+)$ (usually denoted additively with neutral element 0) together with a scalar multiplication $\mathbf{R} \times Q \to Q$ such that the usual unitary $\mathbf{R}$–modules equations are satisfied (i.e., $r(x+y) = rx + ry$, $(r+s)x = rx + sx$, $(rs)x = r(sx)$, $1x = x$ and $0x = 0$ for all $r, s \in \mathbf{R}$ and $x, y \in Q$) and, moreover, $rx + (y+z) = (rx+y) + z$ for all $r \in \mathbf{I}$ and $x, y, z \in Q$. The quasimodule Q is said to be *primitive* if $\mathbf{I}Q = 0$. Obviously, if Q is primitive then every subloop of $Q(+)$ is a subquasimodule. See [21], [22], [25], [26], [28] and [29] for more on quasimodules.

1.5 (Ternary algebras) By a *ternary algebra* we mean a module $_{\mathbf{R}}A$ together with a trilinear mapping $\tau : A^{(3)} \to A$ such that the following equations are satisfied:

$$\mathbf{I}\tau = 0\,; \tag{T0}$$

$$\tau(x,x,y) = 0\,; \tag{T1}$$

$$\tau(\tau(x,y,z),u,v) = 0\,; \tag{T2}$$

$$\tau(u,v,\tau(x,y,z)) = 0\,. \tag{T3}$$

If $A = A(+, rx, \tau)$ is a ternary algebra then we put

$$\overline{\tau}(x,y,z) = \tau(x,y,z) + \tau(y,z,x) + \tau(z,x,y)$$

for all $x, y, z \in A$. Further,

$$\mathrm{An}\,(a) = \{a \in A \mid \tau(a,x,y) = \tau(x,y,a) = 0 \text{ for all } x, y \in A\}\,.$$

2. Normal subquasigroups

An equivalence r defined on a quasigroup Q is said to be a *normal congruence* of Q if the following three conditions are satisfied for all $a, b, c, d \in Q$:

$$(a,b) \in r \text{ and } (c,d) \in r \Rightarrow (ac,bd) \in r\,; \tag{C1}$$

$$(a,b) \in r \text{ and } (ac,bd) \in r \Rightarrow (c,d) \in r\,; \tag{C2}$$

$$(c,d) \in r \text{ and } (ac,bd) \in r \Rightarrow (a,b) \in r\,. \tag{C3}$$

(Note that both (C2) and (C3) follow from (C1) for a finite Q.)

2.1 Lemma. *Let a subquasigroup P of a quasigroup Q be a block (or a class) of a normal congruence r of Q. Then:*

(i) *Every block of r is equal to a left coset aP for some $a \in Q$.*
(ii) *Every block of r is equal to a right coset Pb for some $b \in Q$.*
(iii) $(c,d) \in r \Leftrightarrow cP = dP \Leftrightarrow Pc = Pd$.

Proof. Well known and easy. □

Now, a subquasigroup P is said to be *normal* in Q if P is a block of some normal congruence r of Q; then, due to 2.1, r is uniquely determined by P.

2.2 Lemma. *A subquasigroup P of a left distributive quasigroup Q is normal if and only if the following condition is satisfied:*

(C4) *If $a, b, x, y, z \in Q$ are such that $(xa)(yb) = z(ab)$ and if any two of the elements x, y, z are in P then the remaining one is in P.*

Proof. Assume first that P is a block of a normal congruence r of Q. If $x, y \in P$ then $(xb, yb) \in r$, $((xa)(xb), (xa)(yb)) \in r$ and, since $(xa)(xb) = x(ab)$, we get $(x(ab), z(ab)) \in r$. Now, $(x, z) \in r$ by (C3) and consequently $z \in P$. The other cases are similar.

Now, assume that (C4) is true and define a binary relation r on Q by $(a, b) \in r \Leftrightarrow Pa = Pb$. If $(a, b) \in r$, $(c, d) \in r$ and $x \in P$ then $x(ac) = (xa)(xc) = (yb)(zd) = w(bd)$ for suitable $x, y, z \in P$ and $w \in Q$. Using (C4), we get $w \in P$ and the inclusion $Pac \subseteq Pbd$ follows. Quite similarly, $Pbd \subseteq Pac$ and hence $(ac, bd) \in r$ and (C1) is verified. The conditions (C2) and (C3) may be checked in a similar way. Thus r is a normal congruence and P is among the blocks of r due to the definition of r and the fact that P is a subquasigroup of Q. $\square$

2.3 Lemma. *Let P be a subquasigroup of a left distributive quasigroup Q. Then:*

(i) *$P \cdot ab \subseteq Pa \cdot Pb$ and $|P| \leq |Pa \cdot Pb| \leq |P|^2$ for all $a, b \in Q$.*
(ii) *If P is finite then P is normal in Q if and only if $|P| = |Pa \cdot Pb|$ for all $a, b \in Q$.*

Proof. (i) For every $x \in P$, $x \cdot ab = xa \cdot xb \in Pa \cdot Pb$.
(ii) Combine (i) and 2.2. $\square$

A quasigroup Q is called *simple* if Q is non–trivial and id_q, $Q \times Q$ are the only normal congruences of Q.

A quasigroup Q is called *hamiltonian* if every subquasigroup is normal in Q. Clearly, the class of hamiltonian quasigroups is closed under taking subquasigroups and factorquasigroups. Hamiltonian groups serve as first examples of hamiltonian quasigroups and the next basic result is almost immediate (as in the subcase of abelian groups).

2.4 Proposition. *Every medial quasigroup is hamiltonian.*

Proof. If P is a subquasigroup of a medial quasigroup Q then we define a relation r on Q by $(a, b) \in r \Leftrightarrow Pa = Pb$. Using the medial law, it is straightforward and easy to show that r is a normal congruence of Q and P is one of the blocks. $\square$

2.5 Remark. (i) Because of technical reasons, we prefer to include abelian groups into the class of hamiltonian groups.
(ii) Hamiltonian loops were studied in [38] (see also [10]).
(iii) Quasigroups linear over abelian groups (see [23], [24]) are hamiltonian and play the rôle of abelian groups among hamiltonian quasigroups.

2.6 Proposition. *Let Q be a left distributive quasigroup and let $a \in Q$ be any element. The following conditions are equivalent:*

(i) *For every $x \in Q$, $x \neq a$, the subquasigroup generated by the elements a, x is normal in Q.*
(ii) *Every two–generated subquasigroup is normal in Q.*
(iii) *Q is hamiltonian.*

Proof. (i) $\Rightarrow$ (ii). Let $u, v \in Q$, $u \neq v$, and $P = \langle u, v\rangle$. Since Q is a quasigroup, there exist $b, x \in Q$ such that $ba = u$ and $bx = v$. Then $a \neq x$ and $S = \langle a, x\rangle$ is a normal subquasigroup of Q by (i). On the other hand, the left translation $L_b : y \mapsto by$ is an automorphism of Q and hence $P = L_b(S)$ is normal in Q, too.
(ii) $\Rightarrow$ (iii). We are going to check the condition (C4) for a subquasigroup P of Q (see 2.2). Let $a, b, x, y, z \in Q$ be such that $(xa)(yb) = z(ab)$ and $x, y \in P$ (the other two cases are similar). If $P_1 = \langle x, y\rangle$ then $P_1 \subseteq P$ and P_1 is either trivial or two–generated. Thus P_1 is normal in Q, $z \in P_1$ by (C4) for P_1 and, finally, $z \in P$.
(iii) $\Rightarrow$ (i). This implication is trivial. $\square$

2.7 Corollary. *Let Q be a finite distributive quasigroup and let $a \in Q$. Then Q is hamiltonian if and only if $|\langle x, a\rangle| = |\langle x, a\rangle a_1 \cdot \langle x, a\rangle b_1|$ for all $x, a_1, b_1 \in Q$, $x \neq a$, $a_1 \neq b_1$.* $\square$

3. Two examples

3.1 ([9], [17]) Put $\mathcal{D}_1 = \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and define an operation $\triangle$ on $\mathcal{D}_1$ by

$$\begin{aligned} a \triangle b = (&2a(0) + 2b(0) + a(1)a(3)b(2) + 2a(2)a(3)b(1) + 2a(1)b(2)b(3) \\ &+ a(2)b(1)b(3), 2a(1) + 2b(1), 2a(2) + 2b(2), 2a(3) + 2b(3)) \end{aligned}$$

for all $a = (a(0), a(1), a(2), a(3)) \in \mathcal{D}_1$ and $b = (b(0), b(1), b(2), b(3)) \in \mathcal{D}_1$. One may check easily that $\mathcal{D}_1(\triangle)$ is a symmetric distributive quasigroup (and hence a CH–quasigroup) of order 81. On the other hand, if $x = (0, 0, 0, 0)$, $y = (0, 1, 0, 0)$, $u = (0, 0, 1, 0)$ and $v = (0, 0, 0, 1)$ then

$$(x \triangle y) \triangle (u \triangle v) = (1, 1, 1, 1) \neq (2, 1, 1, 1) = (x \triangle u) \triangle (y \triangle v)\,,$$

and so $\mathcal{D}_1(\triangle)$ is not medial.

Furthermore, $\mathcal{P} = \{(0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 0, 2)\}$ is a three–element subquasigroup of $\mathcal{D}_1(\triangle)$ and the set $(\mathcal{P} \triangle (0, 0, 1, 0)) \triangle (\mathcal{P} \triangle (0, 1, 0, 0))$ contains just 9 elements. In view of 2.7, $\mathcal{P}$ is not normal in $\mathcal{D}_1(\triangle)$.

3.2 Put $\mathcal{D}_2 = \mathbb{Z}_{27} \times \mathbb{Z}_9 \times \mathbb{Z}_3$ and define an operation $\triangledown$ on $\mathcal{D}_2$ by

$$\begin{aligned} a \triangledown b = (&26a(0) + 3a(1) + 2b(0) + 24b(1) + 18a(0)a(2)b(1) + 9a(0)b(1)b(2) \\ &+ 18a(1)b(0)b(2) + 9a(1)a(2)b(0), 8a(1) + 3a(2) + 2b(1) + 6b(2), 2a(2) + 2b(2)) \end{aligned}$$

for all $a = (a(0), a(1), a(2)) \in \mathcal{D}_2$ and $b = (b(0), b(1), b(2)) \in \mathcal{D}_2$. Again, a tedious but straightforward calculation shows that $\mathcal{D}_2$ is a distributive quasigroup of order 729 and $\mathcal{D}_2$ is not medial, since

$$(x \triangledown y) \triangledown (u \triangledown v) = (7, 5, 1) \neq (25, 5, 1) = (x \triangledown u) \triangledown (y \triangledown v)\,,$$

where $x = (0, 0, 0)$, $y = (1, 0, 0)$, $u = (0, 1, 0)$, $v = (0, 0, 1)$. Finally, using 2.6 with $a = (0, 0, 0)$ and 2.2 or 2.7, one may also (at least in principle) show that $\mathcal{D}_2(\triangledown)$ is hamiltonian. Nevertheless, this property is a consequence of 12.8.

4. Commutative Moufang loops

Let $Q = Q(+)$ be a commutative Moufang loop, the operation being denoted additively. The set

$$\mathrm{Z}(Q) = \{a \in Q \mid (a+x)+y = a+(x+y) \text{ for all } x,y \in Q\}$$

is a normal subloop of Q, called the *centre* of Q. The loop Q is said to be *nilpotent of class at most 0* if it is trivial, *of class at most 1* if it is an (abelian) group and *of class at most* $n \geq 2$ if the factorloop $Q/\mathrm{Z}(Q)$ is nilpotent of class at most $n-1$. Further, Q is *nilpotent of class* n if it nilpotent of class at most n and is not nilpotent of class at most $n-1$. The smallest normal subloop P of Q such that the corresponding factorloop Q/P is associative is called the *associator subloop* of Q and is denoted by $P = \mathrm{A}(Q)$ in the sequel. For all $a,b,c \in Q$, the element $[a,b,c] = ((a+b)+c)-(a+(b+c))$ is called the *associator* of a,b,c. Clearly, $\mathrm{A}(Q)$ is just the subloop generated by all associators.

4.1 Proposition. ([10]) (i) *Both* $\mathrm{A}(Q)$ *and* $Q/\mathrm{Z}(Q)$ *are 3-elementary loops* (i.e., they satisfy the equation $3x = 0$).
(ii) *Q is diassociative* (i.e., any two elements generate a subgroup).
(iii) *If $a,b,c \in Q$ are such that $a+(b+c) = (a+b)+c$ then these elements generate a subgroup.*
(iv) *If Q is generated by $n \geq 2$ elements then it is nilpotent of class at most $n-1$.*
(v) *Q is locally nilpotent.*
(vi) *If Q is simple then it is an abelian group of finite prime order.*
(vii) *If Q is finite and not associative then the order of Q is divisible by 81.* □

4.2 Remark. It is proven in [4], [34] and [45] that the free commutative Moufang loop of rank $n \geq 2$ is nilpotent of class $n-1$.

A transformation f of Q is said to be *central* (more precisely, *n–central*) if there exists $n \in \mathbb{Z}$ such that $f(x) + nx \in \mathrm{Z}(Q)$ for every $x \in Q$.

4.3 Lemma. ([29]) *Let f be a transformation of Q. Then:*

(i) *If $m,k \in \mathbb{Z}$, $0 \leq m \leq 2$ and $n = 3k+m$ then f is n–central if and only if it is m–central.*
(ii) *If Q is non–associative and f is central then there is just one $r \in \mathbb{Z}$ such that $0 \leq r \leq 2$ and f is r–central.* □

4.4 Lemma. ([29]) *Let f and g be endomorphisms of Q such that f and g are m–central and n–central, respectively. Then:*

(i) *fg is $(-mn)$–central.*
(ii) *$f+g$ is an $(m+n)$–central endomorphism.*
(iii) *If f is an automorphism then f^{-1} is m–central.* □

4.5 Remark. Assume that Q is not associative. By 4.3 and 4.4, the set $\mathrm{Cend}(Q)$ of central endomorphisms of Q is an associative ring with unit and, for every $f \in \mathrm{Cend}(Q)$, there is a uniquely determined $\Phi(f) \in \mathbb{Z}_3$ such that f is $(-\Phi(f))$–central. Now, the mapping $\Phi : \mathrm{Cend}(Q) \to \mathbb{Z}_3$ is a projective ring homomorphism and $\mathrm{Ker}(\Phi) = \{f \mid f(Q) \subseteq \mathrm{Z}(Q)\}$.

5. Quasimodules

Throughout this section, let Q be a quasimodule, the underlying commutative Moufang loop of Q being denoted by $Q(+)$. A subquasimodule P of Q is *normal* if P is a block of a congruence of Q. If Q is finitely generated then $\mathrm{gen}(Q)$ is the smallest number of generators of Q.

5.1 Proposition. ([21]) (i) *A subquasimodule P of Q is normal if and only if $P(+)$ is a normal subloop of $Q(+)$.*

(ii) *$\mathrm{A}(Q)$ is a normal primitive subquasimodule of Q and $Q/\mathrm{A}(Q)$ is a module.*

(iii) *$\mathrm{Z}(Q)$ is a normal submodule of Q and $Q/\mathrm{Z}(Q)$ is a primitive quasimodule.*

(iv) *If P is a subquasimodule of Q such that either $\mathrm{A}(Q) \subseteq P$ or $P \subseteq \mathrm{Z}(Q)$ then P is a normal subquasimodule of Q.*

(v) *For all $x, y \in Q$, the set $\mathbf{R}x + \mathbf{R}y$ is a submodule of Q and it is just the subquasimodule generated by x, y.*

(vi) *If $a + (b + c) = (a + b) + c$ for some $a, b, c \in Q$ then the subquasimodule generated by these elements is a submodule.*

(vii) *If Q is simple (i.e., if $Q \neq 0$ and $0, Q$ are the only normal subquasimodules of Q) then Q is a module (and hence $0, Q$ are the only submodules of Q).* □

A *preradical* ϱ (for the category of quasimodules) is a subfunctor of the identity functor, i.e., ϱ assigns to each quasimodule Q its subquasimodule $\varrho(Q)$ in such a way that $f(\varrho(Q)) \subseteq \varrho(P)$ whenever P is a quasimodule and $f : Q \to P$ is a homomorphism. Obviously, $\varrho(Q)$ is a normal subquasimodule of Q. A preradical ϱ is said to be *hereditary* if $\varrho(P) = P \cap \varrho(Q)$ for every quasimodule Q and its subquasimodule P, and it is said to be a *radical* if $\varrho(Q/\varrho(Q)) = 0$ for every quasimodule Q.

Let ϱ be a preradical. For every quasimodule Q and every ordinal α we put ${}^0\varrho(Q) = 0$, ${}^{\alpha+1}\varrho(Q)/{}^{\alpha}\varrho(Q) = \varrho(Q/{}^{\alpha}\varrho(Q))$, ${}^{\alpha}\varrho(Q) = \bigcup_{\beta<\alpha} {}^{\beta}\varrho(Q)$ for α limit, and $\widehat{\varrho}(Q) = \bigcup {}^{\alpha}\varrho(Q)$. Then ${}^{\alpha}\varrho$, $\widehat{\varrho}$ are preradicals which are hereditary if ϱ is hereditary, and $\widehat{\varrho}$ is the least radical containing ϱ (see [21]).

Let $\mathrm{K}(Q)$ denote the greatest primitive subquasimodule of Q and $\mathrm{S}(Q) = \mathrm{Soc}(Q)$ the socle of Q (i.e., the subquasimodule generated by all minimal submodules). Then we have $\mathrm{A}(Q) \subseteq \mathrm{K}(Q) \subseteq \mathrm{S}(Q)$. Moreover, both K and S are hereditary preradicals for the category of quasimodules. Now, $\widehat{\mathrm{K}}$ and $\widehat{\mathrm{S}}$ will denote the smallest hereditary radical containing K and S, respectively.

5.2 Lemma. *Let P be a subquasimodule of Q. Then:*

(i) *If $P \cap \mathrm{Z}(Q) = 0$ then $P \subseteq \mathrm{K}(Q)$.*

(ii) *If P is cyclic and $P \cap \mathrm{Z}(Q) = 0$ then either $P = 0$ or $P \simeq \mathbf{P}$.*

(iii) *If $P \neq 0$ is normal and cyclic then $P \cap \mathrm{Z}(Q) \neq 0$ and, moreover, if P is simple then $P \subseteq \mathrm{Z}(Q)$.*

Proof. (i) P is isomorphic to a subquasimodule of $Q/\mathrm{Z}(Q)$, and hence P is primitive by 5.1(iii).

(ii) By (i), P is a cyclic K–torsion module.

(iii) Assume on the contrary that $P \cap \mathrm{Z}(Q) = 0$. By (ii), P contains just three elements, so that $P = \{0, a, -a\}$, $a \neq 0$. Now, for $x, y \in Q$, put $z = [x, y, a] = ((x + y) + a) - (x + (y + a))$. Since P is normal in Q, we have $z \in P$. If $z = a$ then $(x+y)+a = (x+(y+a))+a$, $x+y = x+(y+a)$, $y = y+a$ and $a = 0$, a contradiction. If $z = -a$ then $x + (y + a) = ((x + y) + a) + a = (x + y) + 2a = (x + a) + (y + a)$,

$x = x+a$ and $a = 0$, again a contradiction. Thus $z = 0$ and $(x+y)+a = x+(y+a)$. This means $a \in \mathrm{Z}(Q)$, a final contradiction. $\square$

5.3 Lemma. ([25]) *Assume that Q is not associative and* $\mathrm{gen}(Q) = 3$. *Then:*

(i) $\mathrm{A}(Q) \simeq \mathbf{P}$ *and* $Q/\mathrm{Z}(Q) \simeq \mathbf{P}^{(3)}$.
(ii) *If P is a proper subquasimodule of Q with* $\mathrm{Z}(Q) \subseteq P$ *then P is a module.*
(iii) *If P is a non–associative subquasimodule of Q then* $\mathrm{A}(Q) \subseteq P$ *and P is normal in Q.*
(iv) *If Q is* $\widehat{\mathrm{K}}$*–torsion then every proper subquasimodule of Q is a module.* $\square$

The quasimodule Q is said to be *nilpotent of class at most* $n \geq 0$ if so is the underlying commutative Moufang loop $Q(+)$.

5.4 Proposition. ([21]) *Assume that Q is finitely generated. Then:*

(i) *If* $\mathrm{gen}(Q) = n \geq 2$ *then Q is nilpotent of class at most $n-1$.*
(ii) *Q is noetherian* (i.e., every subquasimodule of Q is finitely generated). $\square$

5.5 Lemma. *Assume that Q is subdirectly irreducible and nilpotent of class 2. Then* $\mathrm{A}(Q) \simeq \mathbf{P}$ *and every proper factorquasimodule of Q is a module.*

Proof. Since $0 \neq \mathrm{A}(Q) \subseteq \mathrm{Z}(Q)$, $\mathrm{A}(Q)$ is a subdirectly irreducible primitive module and consequently $\mathrm{A}(Q) \simeq \mathbf{P}$. $\square$

5.6 Proposition. *Assume that Q is* $\widehat{\mathrm{K}}$*–torsion and not associative. The following conditions are equivalent:*

(i) *Q is subdirectly irreducible and* $\mathrm{gen}(Q) = 3$.
(ii) *Every proper factorquasimodule as well as every proper subquasimodule of Q is a module.*

Proof. (i) $\Rightarrow$ (ii). By 5.4(i), Q is nilpotent of class 2 and we can use 5.5 and 5.3(iv). (ii) $\Rightarrow$ (i). Since Q is not associative, we have $(a+b)+c \neq a+(b+c)$ for some $a, b, c \in Q$ and it is clear that Q is generated by these elements. Thus $\mathrm{gen}(Q) = 3$. The fact that Q is subdirectly irreducible is also clear. $\square$

5.7 Lemma. *Assume that Q is finitely generated and let P be a (proper) maximal subquasimodule of Q. Then P is normal in Q.*

Proof. We shall proceed by induction on the nilpotence class n of Q (see 5.4(i)). First, the result is clear for $n \leq 1$ and if $\mathrm{Z}(Q) \subseteq P$ then $P/\mathrm{Z}(Q)$ is normal in $Q/\mathrm{Z}(Q)$ by induction. Thus P is normal in Q in this case and we may assume that $\mathrm{Z}(Q) \nsubseteq P$. But then $Q = P + \mathrm{Z}(Q)$ and it is easy to check directly that P is normal in Q. $\square$

If Q is finitely generated then $\mathrm{J}(Q)$ will denote the intersection of all maximal submodules of Q.

5.8 Proposition. *Assume that Q is finitely generated. Then:*

(i) $\mathrm{J}(Q)$ *is a normal subquasimodule of Q and* $\mathrm{A}(Q) \subseteq \mathrm{J}(Q)$.
(ii) $\mathrm{gen}(Q) = \mathrm{gen}(Q/\mathrm{J}(Q)) = \mathrm{gen}(Q/\mathrm{A}(Q))$.
(iii) *If Q is* $\widehat{\mathrm{K}}$*–torsion then* $Q/\mathrm{J}(Q)$ *is primitive and* $|Q/\mathrm{J}(Q)| = 3^{\mathrm{gen}(Q)}$.

Proof. By 5.7 and 5.1(vii), $\mathrm{J}(Q)$ is a normal subquasimodule and $\mathrm{A}(Q) \subseteq \mathrm{J}(Q)$. The inequalities $n = \mathrm{gen}(Q) \geq \mathrm{gen}(Q/\mathrm{A}(Q)) \geq \mathrm{gen}(Q/\mathrm{J}(Q))$ are clear. Now, let N be a generator set of Q, $|N| = n$, and let M be a subset of Q such that $Q/\mathrm{J}(Q)$ is generated by $M/\mathrm{J}(Q)$. We claim that Q is generated by M.

Assume the contrary and consider a subset N_1 of N maximal with respect to the property that Q is not generated by $M \cup N_1$. Then $N_1 \neq N$ and we take $v \in N \setminus N_1$. Further, consider a subquasimodule V of Q maximal with respect to $M \cup N_1 \subseteq V$ and $v \notin V$. It is easy to see that V is a maximal subquasimodule of Q, and hence $\mathrm{J}(Q) \subseteq V$ and $V = Q$, a contradiction.

We have shown that M generates Q and it follows easily that $\mathrm{gen}(Q/\mathrm{J}(Q)) = \mathrm{gen}(Q)$.

Now, finally, assume that Q is $\widehat{\mathrm{K}}$–torsion. Then every simple factor of Q is a copy of $\mathbf{P}$ and $Q/\mathrm{J}(Q)$ is a primitive module which is a direct sum of n copies of $\mathbf{P}$. $\square$

5.9 Lemma. *If Q is finitely generated and $\widehat{\mathrm{K}}$–torsion then $\mathbf{I}Q \subseteq \mathrm{J}(Q) \cap \mathrm{Z}(Q)$ and $\mathrm{gen}(Q) = \mathrm{gen}(Q/\mathbf{I}Q)$.*

Proof. Use 5.8. $\square$

5.10 Lemma. *Assume that Q is a primitive quasimodule nilpotent of class at most 2 with $\mathrm{gen}(Q) = n$. Then $|Q| \leq 3^{n+m}$, where $m = \binom{n}{3}$.*

Proof. As $Q/\mathrm{A}(Q)$ is a primitive module, its additive group is 3–elementary and every its subgroup is a submodule. By 5.8(ii), $\mathrm{gen}(Q/\mathrm{A}(Q)) = n$, and consequently $|Q/\mathrm{A}(Q)| = 3^n$. If $n \leq 2$ then $\mathrm{A}(Q) = 0$. Now, let $n \geq 3$, $M = \{a_1, \dots, a_n\}$ be a generating set of Q, $N = \{\,[a_i, a_j, a_k] \mid 1 \leq i < j < k \leq n\}$, and P be the subquasimodule generated by N. Then, Q being nilpotent of class at most 2, $P \subseteq \mathrm{A}(Q) \subseteq \mathrm{Z}(Q)$ and P is a normal subquasimodule of Q by 5.1(iv). Denote by f the natural projection of Q onto Q/P. Then $K = \{f(a_1), \dots, f(a_n)\}$ generates Q/P, $x + (y + z) = (x + y) + z$ for all $x, y, z \in K$ and Q/P is associative by 5.1(vi). Thus $\mathrm{A}(Q) = P$, $\mathrm{gen}(\mathrm{A}(Q)) \leq |N| = m$ and $|\mathrm{A}(Q)| \leq 3^m$, since $\mathrm{A}(Q)$ is a primitive module, too. $\square$

5.11 Lemma. *Let P be a minimal submodule of Q, $a, b \in Q$, $A = P + (a + b)$ and $B = (P + a) + (P + b)$. Then:*

- (i) *$A \subseteq B$.*
- (ii) *If P is normal in Q then $A = B$.*
- (iii) *If P is not isomorphic to $\mathbf{P}$ then $A = B$.*
- (iv) *If $A \neq B$ then $P \simeq \mathbf{P}$, $|A| = 3$ and $|B| = 9$.*

Proof. We may assume that P is not normal in Q, $A \neq B$ and Q is generated by $P \cup \{a, b\}$. By 5.2(ii) and 5.4(i), $P \simeq \mathbf{P}$ and Q is nilpotent of class 2. Consequently, $|A| = 3$ and $3 \leq |B| \leq 9$. Now, let $(x + a) + (y + b) = (u + a) + (v + b)$ for some $x, y, u, v \in P$, $x \neq u$, $y \neq v$. Then we have $a + (r + b) = ((x + a) + (y + b)) - 2x = ((u + a) + (v + b)) - 2x = (a + s) + (b + t)$, where $r = y - x$, $s = u - x$, $t = v - x$, $r \neq t$, $s \neq 0$ (the subquasimodules $\langle P, a\rangle$ and $\langle P, b\rangle$ are at most two–generated, and hence they are associative). Furthermore, $\mathrm{A}(Q) \subseteq \mathrm{Z}(Q)$, and therefore $(a + b) + r + \alpha = a + (r + b) = (a + s) + (b + t) = (a + b) + (s + t) + \beta$ for some $\alpha, \beta \in \mathrm{Z}(Q)$. Then $\alpha + r = \beta + (s + t)$, $\alpha - \beta \in P \cap \mathrm{Z}(Q) = 0$ (since P is minimal and not normal in Q), $\alpha = \beta$ and $r = s + t$. Thus $a + (b + r) = (a + s) + (b + t)$, where $r = s + t$ and $s \neq 0$. If $r = 0$ then $(a + b) + 2s = ((a + s) + (b - s)) + 2s = (a + 2s) + b$ and

$Q = \langle a, b, 2s\rangle$ is associative, a contradiction. Similarly if $t = 0$. Finally, if $r \neq 0 \neq t$ then $t = s$ and $a + (b + r) = (a + b) + 2s = (a + b) + r$, again a contradiction. $\square$

5.12 Remark. Let P be a minimal submodule of Q. Then, for every $a \in Q$, the subquasimodule $\langle P, a\rangle$ is at most two–generated, and so it is a submodule and $P+(P+a) = P+a$. By 5.11, P is normal in Q if and only if $|P|\cdot|(P+a)+(P+b)| \neq 27$ for all $a, b \in Q$.

6. Ternary representations of quasimodules nilpotent of class at most 2

Throughout this section, the word *quasimodule* always means *quasimodule nilpotent of class at most 2.*

6.1 Proposition. *Let $A = A(+, rx, \tau)$ be a ternary algebra. Then $\mathrm{q}(A) = A(\circledast, rx)$ is a quasimodule, where the underlying commutative Moufang loop is defined by*

$$x \circledast y = x + y + \tau(x, y, x - y)$$

for all $x, y \in A$. Moreover, $\mathrm{Z}(A(\circledast)) = \{a \in A \,|\, \overline{\tau}(a, x, y) = 0$ for all $x, y \in A\}$ and $\mathrm{A}(A(\circledast))$ is the subloop generated by $\mathrm{Im}(\overline{\tau})$.

Proof. Clearly, 0 is the neutral element of $A(\circledast)$ and $x \circledast y = x + y + \tau(x, y, x) + \tau(y, x, y) = y \circledast x$. Further, $(x \circledast x) \circledast (y \circledast z) = 2x + y + z + \tau(x, y, x) + \tau(x, y, y) + \tau(x, z, x)+\tau(x, z, z)+\tau(y, z, y)+\tau(z, y, z)+\tau(x, y, z)+\tau(x, z, y) = (x\circledast y)\circledast(x\circledast z)$ for all $x, y, z \in A$. If $x \circledast y = x \circledast z$ then $y + \tau(x, y, x) + \tau(y, x, y) = v = z + \tau(x, z, x) + \tau(z, x, z)$, and hence $\tau(x, y, x) = \tau(x, v, x) = \tau(x, z, x)$, $\tau(y, x, y) = \tau(v, x, v) = \tau(x, z, x)$ and $y = z$. Finally, if $z = y - x + \tau(x, y, x) + \tau(x, y, y)$ then $x \circledast z = y$. We have checked that $A(\circledast)$ is a commutative Moufang loop. The opposite (or inverse) element to x is $-x$ and $x \ominus y = x \circledast (-y) = x - y + \tau(y, x, x) + \tau(y, x, y)$. Now, for all $a, x, y \in A$, we have $[a, x, y] = ((a \circledast x) \circledast y) \ominus (a \circledast (x \circledast y)) = \overline{\tau}(a, x, y)$. Consequently, $\mathrm{Z}(A(\circledast)) = \{a \,|\, \overline{\tau}(a, x, y) = 0\}$ and it is clear that $\mathbf{I}A \subseteq \mathrm{Z}(A(\circledast))$.

For every $r \in \mathbf{R}$, $r^3 - r \in \mathbf{I}$, and hence $r(x \circledast y) = rx + ry + r\tau(x, y, x - y) = rx + ry + r^3\tau(x, y, x - y) = rx \circledast ry$. Similarly, $(r + s)x = rx + sx = rx + sx + \tau(rx, sx, rx - sx) = rx \circledast sx$ and we see that $A(\circledast, rx)$ is a quasimodule. It remains to show that this quasimodule is nilpotent of class at most 2. However, $((x \circledast y) \circledast z) \ominus (x \circledast (y \circledast z)) \in \mathrm{Z}(A(\circledast))$ for all $x, y, z \in A$ and the rest is clear. $\square$

Quasimodules $\mathrm{q}(A)$, A being a ternary algebra, will be said to have *ternary representation*. Now, we are going to show that every free quasimodule of finite rank has a ternary representation.

6.2 Let $n \geq 2$, $m = \binom{n}{3}$, $q = n + m$, and $F = F_n = \mathbf{R}^{(n)} \times \mathbf{P}^{(m)}$. Then F is an $\mathbf{R}$–module and the elements $a_1 = (1, 0, \dots, 0), \dots, a_q = (0, \dots, 0, 1)$ form a canonical set M of generators of F. Let K be the set of ordered triples (i, j, k), $1 \leq i < j < k \leq n$, and let $f : K \to \{1, \dots, m\}$ be a bijection. Now, define a mapping $\sigma : M^{(3)} \to F$ by $\sigma(a_i, a_j, a_k) = a_{n+f(\alpha)}$, $\sigma(a_j, a_i, a_k) = 2a_{n+f(\alpha)}$ for every $\alpha = (i, j, k) \in K$ and $\sigma(a_i, a_j, a_k) = 0$ for every triple (i, j, k) such that neither (i, j, k) nor (j, i, k) is in K. Then this mapping σ can be extended (in a unique way) to a trilinear mapping $\tau : F^{(3)} \to F$ and $F = F(+, rx, \tau)$ becomes a ternary algebra. Now, consider the corresponding quasimodule $\mathrm{q}(F) = F(\circledast, rx)$ (see 6.1).

6.2.1 Proposition. *$\mathrm{q}(F)$ is a free quasimodule and the set $N = \{a_1, \dots, a_n\}$ is a free basis of $\mathrm{q}(F)$. Moreover, $\mathrm{A}(F(\circledast)) = \mathbf{P}^{(m)}$, $\mathrm{Z}(F(\circledast)) = \mathbf{I}^{(n)} \times \mathbf{P}^{(m)}$ and $\mathbf{I}F = \mathbf{I}^{(n)}$.*

Proof. We have $((a_i \circledast a_j) \circledast a_k) \ominus (a_i \circledast (a_j \circledast a_k)) = a_{n+f(\alpha)}$ for every $\alpha = (i, j, k) \in K$. Consequently, the quasimodule $q(F)$ is generated by N. The equalities $\mathrm{A}(F(\circledast)) = \mathbf{P}^{(m)}$, $\mathrm{Z}(F(\circledast)) = \mathbf{I}^{(n)} \times \mathbf{P}^{(m)}$ and $\mathbf{I}F = \mathbf{I}^{(n)}$ are also easy to check. It remains to show that $\mathrm{q}(F)$ is free over N.

Now, let $E = E(\circledast, rx)$ be the free quasimodule over N and let $\pi : E \to \mathrm{q}(F)$ be the (unique) projective quasimodule homomorphism such that $\pi \restriction N = \mathrm{id}_N$. Then $\pi(\mathrm{A}(E)) = \mathrm{A}(\mathrm{q}(F))$, $\pi(\mathbf{I}E) = \mathbf{I}F$ and π induces projective homomorphisms $\varphi : E/\mathrm{A}(E) \to \mathrm{q}(F)/\mathrm{A}(\mathrm{q}(F))$ and $\psi : E/\mathbf{I}E \to \mathrm{q}(F)/\mathbf{I}F$ such that $\varphi\lambda = \varrho\pi$ and $\psi\mu = \nu\pi$, where $\lambda, \varrho, \mu, \nu$ are the corresponding natural projections. Moreover, $\varphi\lambda(N) = \varrho\pi(N) = \varrho(N)$ is a free basis of the free module $\mathrm{q}(F)/\mathrm{A}(\mathrm{q}(F))$, $|\lambda(N)| = |\varphi\lambda(N)| = |\varrho(N)| = |N| = n$ and we conclude that φ is an isomorphism and $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(\lambda) = \mathrm{A}(E)$. On the other hand, $|\mathrm{q}(F)/\mathbf{I}F| = 3^q$ and $E/\mathbf{I}E$ is a free primitive quasimodule of rank n. By 5.10, $|E/\mathbf{I}E| \leq 3^q$, and therefore ψ is also an isomorphism and $\mathrm{Ker}(\pi) \subseteq \mathrm{Ker}(\mu) = \mathbf{I}E$. We have shown that $\mathrm{Ker}(\pi) \subseteq \mathrm{A}(E) \cap \mathbf{I}E$ and to finish the proof it suffices to check that $\mathrm{A}(E) \cap \mathbf{I}E = 0$.

First, take $a \in \mathbf{I}E$. Since $\mathbf{I}E \subseteq \mathrm{Z}(E)$ and N is a free basis of E, we have $a = r_1 a_1 \circledast \dots \circledast r_n a_n$ for some $r_1, \dots, r_n \in \mathbf{R}$. Now, if $a \in \mathrm{A}(E)$ then $0 = \lambda(a) = r_1\lambda(a_1) \circledast \dots \circledast r_n\lambda(a_n)$. But $E/\mathrm{A}(E)$ is a free module over $\{\lambda(a_1), \dots, \lambda(a_n)\}$, and hence $r_1 = \dots = r_n = 0$ and $a = 0$. □

6.2.2 Lemma. *$\tau \restriction Z \times F \times F = \tau \restriction F \times Z \times F = \tau \restriction F \times F \times Z = 0$, where $Z = \mathrm{Z}(F(\circledast))$.*

Proof. Obvious. □

6.2.3 Corollary. *Every submodule of $\mathrm{Z}(F(\circledast))$ is an ideal of the ternary algebra F.* □

6.3 Proposition. *Every finite $\widehat{\mathrm{K}}$–torsion quasimodule has ternary representation.*

Proof. Let $Q = Q(\circledast, rx)$ be a finite $\widehat{\mathrm{K}}$–torsion quasimodule which is not a module. Then $n = \mathrm{gen}(Q) \geq 3$ and there exists a projective homomorphism $\pi : \mathrm{q}(F) \to Q$ as it follows from 6.2.1; put $G = \mathrm{Ker}(\pi) \circledast \mathbf{I}F$. Then G is a normal subquasimodule of $\mathrm{q}(F)$ and $\varphi(G)$ is a normal subquasimodule of $H = \mathrm{q}(F)/\mathbf{I}F$, $\varphi : \mathrm{q}(F) \to H$ being the natural projection. Moreover, $H_1 = H/\varphi(G) \simeq Q/\mathbf{I}Q$ and, by 5.8 and 5.9, $n = \mathrm{gen}(Q/\mathbf{I}Q) = \mathrm{gen}(H_1) = \mathrm{gen}(H_1/\mathrm{A}(H_1))$. Consequently, $H_1/\mathrm{A}(H_1)$ is a primitive module of dimension n and $|H_1/\mathrm{A}(H_1)| = 3^n$. Since $H_1/\mathrm{A}(H_1) \simeq H/L$, where $L = \varphi(G) \circledast \mathrm{A}(H)$, we have also $|H/L| = 3^n$. On the other hand, $|H/\mathrm{A}(H)| = 3^n$, $\mathrm{A}(H) = L$, $\varphi(G) \subseteq \mathrm{A}(H)$ and $\mathrm{Ker}(\pi) \subseteq \mathrm{A}(\mathrm{q}(F)) \circledast \mathbf{I}F = \mathrm{Z}(\mathrm{q}(F))$ (see 6.2.1). Now, by 6.2.3, $\mathrm{Ker}(\pi)$ is an ideal of the ternary algebra F and it suffices to consider the corresponding factoralgebra. □

6.4 Remark. Using primary decompositions (and filtered products), one may show that every finite $\widehat{\mathrm{S}}$–torsion quasimodule has ternary representation (and that every $\widehat{\mathrm{S}}$–torsion quasimodule is imbeddable into a quasimodule with ternary representation).

7. Hamiltonian quasimodules

A quasimodule Q is said to be *hamiltonian* if every subquasimodule is normal in Q. Clearly, every module is hamiltonian and the class of hamiltonian quasimodules is closed under subquasimodules and factorquasimodules.

A quasimodule Q is said to be *cocyclic* if $\mathrm{S}(Q)$ is a non–zero essential simple submodule of Q.

7.1 Proposition. *Let Q be a cocyclic quasimodule. Then:*

- (i) *Q is subdirectly irreducible, hamiltonian and nilpotent of class at most 2.*
- (ii) *If Q is non–associative then $\mathrm{A}(Q) = \mathrm{S}(Q) \simeq \mathbf{P}$ and every proper factorquasimodule of Q is a module.*

Proof. Clearly, $\mathrm{S}(Q)$ is the smallest non–zero normal subquasimodule, and hence Q is subdirectly irreducible. Now, we may assume that Q is not associative. Then $\mathrm{A}(Q) \subseteq \mathrm{S}(Q)$ implies $\mathrm{A}(Q) = \mathrm{S}(Q) \simeq \mathbf{P}$ and $\mathrm{A}(Q) \subseteq \mathrm{Z}(Q)$ (see 5.2(iii) and 5.5). Thus Q is hamiltonian and nilpotent of class at most 2. $\square$

7.2 Lemma. *If Q is a non–associative hamiltonian quasimodule then $\mathrm{A}(Q) \subseteq \mathrm{K}(Q) \subseteq \mathrm{S}(Q) \subseteq \mathrm{Z}(Q)$.*

Proof. Use 5.2(iii). $\square$

7.3 Corollary. *Every hamiltonian primitive quasimodule is a module.* $\square$

7.4 Proposition. *A non–zero quasimodule is cocylic if and only if it is hamiltonian and subdirectly irreducible.*

Proof. Use 7.1. $\square$

7.5 Proposition. *Let Q be a non–associative cocyclic quasimodule. Then Q is $\widehat{\mathrm{K}}$–torsion. Moreover, if Q is finitely generated then it is finite and $|Q| = 3^n$ for some $n \geq 4$.*

Proof. By 7.1, $\mathbf{P} \simeq \mathrm{A}(Q) = \mathrm{S}(Q) \subseteq \mathrm{Z}(Q)$. Since $\mathbf{R}$ is a commutative noetherian ring, every hereditary radical (for $\mathbf{R}$–Mod) is stable, and hence, in particular, $\mathrm{Z}(Q)$ is $\widehat{\mathrm{K}}$–torsion. On the other hand, the factor $Q/\mathrm{Z}(Q)$ is primitive, thus being K–torsion. Consequently, Q is $\widehat{\mathrm{K}}$–torsion.

Now, assume that Q is finitely generated. By 5.4(ii), Q is a noetherian quasimodule, Q has a finite K–sequence and we may restrict ourselves to the case when Q is K–torsion. Then both $\mathrm{Z}(Q)$ and $Q/\mathrm{Z}(Q)$ are noetherian primitive modules, thus being finite direct sums of copies of $\mathbf{P}$ and the rest is clear. $\square$

7.6 Proposition. *Let Q be a non–associative hamiltonian quasimodule. Then there exist a subquasimodule Q_1 of Q and a (normal) subquasimodule Q_2 of Q_1 such that the factor $Q_3 = Q_1/Q_2$ is non–associative, cocyclic, $\widehat{\mathrm{K}}$–torsion, $\mathrm{gen}(Q_3) = 3$ and $|Q_3| = 3^n$ for some $n \geq 4$.*

Proof. Since Q is not associative, there is a non–associative subquasimodule Q_1 of Q such that $\mathrm{gen}(Q_1) = 3$. Further, there is a subquasimodule Q_2 of Q_1 such that $Q_3 = Q_1/Q_2$ is subdirectly irreducible and non–associative. Now, $\mathrm{gen}(Q_3) = 3$ and Q_3 is cocyclic by 7.4. $\square$

7.7 Theorem. *A finite quasimodule Q is non–associative and cocyclic if and only if there exists a ternary algebra A such that $Q = \mathrm{q}(A)$ (see 6.1), $\overline{\tau} \neq 0$ and the underlying module $A' = A(+, rx)$ is cocyclic (in this case, A' is $\widehat{\mathrm{K}}$–torsion and $\mathrm{gen}(A') \geq 3$).*

Proof. Assume first that Q is both non–associative and cocyclic. By 7.1 and 7.5, Q is $\widehat{\mathrm{K}}$–torsion and nilpotent of class 2. By 6.3, Q has a ternary representation $Q = \mathrm{q}(A)$. Now, the quasimodule $\mathrm{q}(A)$ and the module A' have the same cyclic submodules and it follows easily that A' is cocyclic and $\widehat{\mathrm{K}}$–torsion,. Further, by 6.1, we have $\overline{\tau} \neq 0$ and one may check easily that then $\mathrm{gen}(A') \geq 3$.

Now, the converse implication. Again, since $\mathrm{q}(A)$ and A' have the same cyclic submodules, $\mathrm{q}(A)$ is cocyclic. Finally, since $\overline{\tau} \neq 0$, the quasimodule $\mathrm{q}(A)$ is non–associative. $\square$

7.8 Theorem. *There exists a non–associative hamiltonian quasimodule if and only if there exists a finite cocyclic $\widehat{\mathrm{K}}$–torsion module M such that $\mathrm{gen}(M) \geq 3$.*

Proof. The direct implication follows from 7.6 and 7.7 and we have to show the converse one. To that purpose, we may assume that $\mathrm{gen}(M) = 3$. Further, consider the ternary algebra $F = F_3$ constructed in 6.2 and the corresponding free quasimodule $\mathrm{q}(F)$. Let D be a submodule of ${}_{\mathbf{R}}E = \mathbf{R}a_1 + \mathbf{R}a_2 + \mathbf{R}a_3 = \mathbf{R}^{(3)} \subseteq F$ such that $E/B \simeq {}_{\mathbf{R}}M$. Since M is $\widehat{\mathrm{K}}$–torsion, we have $\mathrm{J}(M) = (\mathbf{I}E + B)/B$, and therefore $M/\mathrm{J}(M) \simeq E/(\mathbf{I}E + B)$. Since M is finite and $\mathrm{gen}(M) = 3$, we have $\mathrm{gen}(M/\mathrm{J}(M)) = 3$, and consequently $E/(\mathbf{I}E + B)$ is a K-torsion module of dimension 3 and, in particular, $|E/(\mathbf{I}E + B)| = 27$. On the other hand, $\mathbf{I}E = \mathbf{I}a_1 + \mathbf{I}a_2 + \mathbf{I}a_3$ and $|E/\mathbf{I}E| = 27$, too. Thus $B \subseteq \mathbf{I}E$ and, since $E/\mathbf{I}E$ is not cocyclic, we have $B \neq \mathbf{I}E$ and $A/B \simeq \mathbf{P}$ for a submodule A of $\mathbf{I}E$, $B \subseteq A \subseteq \mathbf{I}E$. Now, fix an epimorphism $\varphi : A \to \mathbf{P}$, $\mathrm{Ker}(\varphi) = B$, and define a subset V of F by $x = (x_1, x_2, x_3, x_4) \in V$ if and only if $f(x) = (x_1, x_2, x_3, 0) \in A$ and $\varphi(f(x)) = x_4$. Then V is a submodule of $\mathbf{I}E + \mathbf{R}a_4$ and, since $\mathbf{I}a_4 = 0$, we have $u \circledast v = u + v$ for all $u, v \in V$. Consequently, V is a subquasimodule of $\mathrm{q}(F)$ and it is easy to check that V is a normal subquasimodule. We denote by Q the corresponding factorquasimodule; clearly $|Q| = 3|M|$. Since $V \cap \mathbf{R}a_4 = 0$, the quasimodule Q is not associative. Furthermore, $P = (\mathbf{R}a_4 + V)/V \simeq \mathbf{P}$ is a normal simple submodule of Q and $Q/P \simeq \mathrm{q}(F)/(\mathbf{R}a_4 + V)$ is a module. Consequently, $P = \mathrm{A}(Q)$ and, in order to show that Q is hamiltonian, it is sufficient to check that P is contained in every non–zero cyclic submodule of Q or, equivalently, that $a_4 \in \mathbf{R}x + V$ for every $x \in F \setminus V$.

Let $x = (x_1, x_2, x_3, x_4) \in F \setminus V$ and $y = f(x) = (x_1, x_2, x_3, 0)$. Since $x \notin V$, we have either $y \in A$ and $\varphi(y) \neq x_4$, or $y \notin A$. In the former case, $z = (x_1, x_2, x_3, \varphi(y)) \in V$, $0 \neq x - z \in \mathbf{R}a_4$, $a_4 = r(x - z)$ for some $r \in \mathbf{R}$ and $a_4 \in \mathbf{R}x + V$.

Assume that $y \notin A$. Since M is finite and $\widehat{\mathrm{K}}$–torsion, there is $m \geq 1$ with $\mathbf{I}^m y \subseteq B$ and $\mathbf{I}^{m-1} y \nsubseteq B$. If $m = 1$ then $y + B \in \mathrm{K}(M) = A/B$ and $y \in A$, a contradiction. Hence $m \geq 2$ and $sy \notin B$ for some $s \in \mathbf{I}^{m-1}$. Now, $sy \in A$ and $sx = (sx_1, sx_2, sx_3, 0)$. Finally, $z = (sx_1, sx_2, sx_3, \varphi(sy)) \in V$ and $z = sx + v$, $v = (0, 0, 0, \varphi(sy)) \in \mathbf{R}a_4$. Thus $v \in \mathbf{R}x + V$ and, since $v \neq 0$, we conclude that $a_4 \in \mathbf{R}x + V$. $\square$

7.9 Remark. If $\mathbf{R}$ is a principal ideal domain then all finitely generated cocyclic modules are cyclic, and hence every hamiltonian ($\mathbf{R}$–)quasimodule is a module.

7.10 Remark. According to [20], [25] and [31], there exists a finite (non–associative) subdirectly irreducible primitive quasimodule of order $n \geq 1$ if and only if $n = 3^m$ for $m \geq 1$, $m \neq 2, 3, 5$ ($m \geq 4$, $m \neq 5$).

8. Trimedial quasigroups

Recall that by a trimedial quasigroup we mean a quasigroup Q such that every subquasigroup P generated by at most three elements is medial (i.e., P satisfies $(ax)(yb) = (ay)(xb)$ identically). We denote by $\mathcal{T}$ the variety (or equational class) of trimedial quasigroups and by $\mathcal{T}^p$ that of pointed trimedial quasigroups ($\mathcal{T}^p$ contains just ordered pairs (Q, a), where $Q \in \mathcal{T}$ and $a \in Q$).

The following basic result is proven in [22] (see also [19]).

8.1 Proposition. *The following conditions are equivalent for a quasigroup Q:*

(i) $Q \in \mathcal{T}$.
(ii) *There exist a commutative Moufang loop $Q(+)$ (defined on the same underlying set as Q), commuting 1-central automorphisms f, g of $Q(+)$ and a central element $a \in \mathrm{Z}(Q(+))$ such that $xy = f(x) + g(y) + a$ for all $x, y \in Q$.* $\square$

In this case, Q is medial iff $Q(+)$ is associative.

The ordered quadruple $(Q(+), f, g, a)$ will be called an *arithmetical form* of the trimedial quasigroup Q. Notice also that Q is medial if and only if $Q(+)$ is an abelian group.

8.2 Lemma. ([22], 3.2, 3.3) *Let $Q \in \mathcal{T}$. Then:*

(i) *For every $w \in Q$ there exists an arithmetical form $(Q(+), f, g, a)$ of Q such that $w = 0$ is the neutral element of the loop $Q(+)$ (then $a = ww$).*
(ii) *If $(Q(+), f, g, a)$ and $Q(*), p, q, b)$ are arithmetical forms of Q such that the loops $Q(+)$ and $Q(*)$ possess the same neutral element then $Q(+) = Q(*)$, $f = p$, $g = q$ and $a = b$.* $\square$

8.3 Lemma. ([22], 3.4) *Let $Q(+), f, g, a)$ and $P(+), p, q, b)$ be arithmetical forms of trimedial quasigroups Q and P, respectively, and let $\varphi : Q \to P$ be a mapping such that $\varphi(0) = 0$. Then φ is a homomorphism of the quasigroups if and only if φ is a homomorphism of the loops such that $\varphi f = p\varphi$, $\varphi g = q\varphi$ and $\varphi(a) = b$.* $\square$

Put $\mathbf{R}_1 = \mathbb{Z}[\mathbf{x}, \mathbf{y}, \mathbf{x}^{-1}, \mathbf{y}^{-1}]$, $\mathbf{x}$ and $\mathbf{y}$ being two commuting indeterminates over the ring $\mathbb{Z}$ of integers. Then $\mathbf{R}_1$ is a commutative noetherian domain, a unique factorization domain, and there exists just one homomorphism $\mathbf{\Phi}$ of $\mathbf{R}_1$ onto $\mathbb{Z}_3$; we have $\mathbf{\Phi}(\mathbf{x}) = 2 = \mathbf{\Phi}(\mathbf{y})$ and $\mathbf{I} = \mathrm{Ker}(\mathbf{\Phi}) = 3\mathbf{R}_1 + (1+\mathbf{x})\mathbf{R}_1 + (1+\mathbf{y})\mathbf{R}_1$. Further, we denote by $\mathcal{Q}_1^c$ the variety of centrally pointed $\mathbf{R}_1$–quasimodules. That is, $\mathcal{Q}_1^c$ contains just ordered pairs $(\overline{Q}, a)$, where $\overline{Q}$ is an $\mathbf{R}_1$–quasimodule and $a \in \mathrm{Z}(\overline{Q})$.

8.4 Proposition. *The varieties $\mathcal{T}^p$ of pointed trimedial quasigroups and $\mathcal{Q}_1^c$ of centrally pointed $\mathbf{R}_1$–quasimodules are equivalent.*

Proof. Let $(Q, w) \in \mathcal{T}^p$. By 8.2(i), there is an arithmetical form $(Q(+), f, g, a)$ of Q such that $w = 0$ is the neutral element of $Q(+)$ and $a = ww \in \mathrm{Z}(Q(+))$. The automorphisms f, g are 1–central, i.e., $x + f(x) \in \mathrm{Z}(Q(+))$ and $x + g(x) \in \mathrm{Z}(Q(+))$ for every $x \in Q$. Furthermore, $3Q \subseteq \mathrm{Z}(Q(+))$ (which is true in every commutative Moufang loop), and consequently we may turn $Q(+)$ into a quasimodule $\overline{Q}$ by

setting $\mathbf{x}x = f(x)$ and $\mathbf{y}x = g(x)$ for every $x \in Q$; clearly, $\mathbf{I}Q \subseteq \mathrm{Z}(\overline{Q})$. Now, $\lambda(Q, w) = (\overline{Q}, a) \in \mathcal{Q}_1^c$.

Conversely, take $(\overline{Q}, a) \in \mathcal{Q}_1^c$ and define a binary operation on Q by $xy = \mathbf{x}x + \mathbf{y}y + a$ for all $x, y \in Q$. By 8.1, Q becomes a trimedial quasigroup and we have $\varkappa(\overline{Q}, a) = (Q, 0) \in \mathcal{T}^p$.

We get correspondences $\lambda : \mathcal{T}^p \to \mathcal{Q}_1^c$, $\varkappa : \mathcal{Q}_1^c \to \mathcal{T}^p$ and it follows easily from 8.2 that $\varkappa\lambda = \mathrm{id}$ and $\lambda\varkappa = \mathrm{id}$. Both correspondences are biunique, they preserve the underlying sets and, in view of 8.3, they represent equivalences between the varieties. $\square$

8.5 Lemma. *Let $\alpha = (Q(+), f, g, a)$ and $\beta = (Q(*), p, q, b)$ be arithmetical forms of a trimedial quasigroup Q (the neutral elements of $Q(+)$ and $Q(*)$ being denoted by 0 and o, respectively) and let $(\overline{Q}, a)$ and $(\widetilde{Q}, b)$ be centrally pointed quasimodules corresponding to α and β, respectively* (see 8.3). *Then the quasimodules $\overline{Q}$ and $\widetilde{Q}$ are isomorphic.*

Proof. Define an operation $\circ$ on Q by $x \circ y = (x+y) - o$ for all $x, y \in Q$. Then $Q(\circ)$ is a loop, o is its neutral element and $h : Q(\circ) \to Q(+)$ is an isomorphism, where $h(x) = x - o$. Moreover, $p_1 = h^{-1}fh$ and $q_1 = h^{-1}gh$ are 1-central automorphisms of $Q(\circ)$, $p_1q_1 = q_1p_1$, $b_1 = f(o) + g(o) + a \in \mathrm{Z}(Q(\circ))$ and $xy = p_1(x) + q_1(y) + b_1$ for all $x, y \in Q$. Now, by 8.2(ii), $Q(\circ) = Q(*)$, $p_1 = p$, $q_1 = q$ and $b_1 = b$, and hence h is an isomorphism of the quasimodules. $\square$

8.6 Proposition. *Let Q be a trimedial quasigroup and let $\overline{Q}$ be the corresponding quasimodule* (see 8.4 and 8.5). *Then:*

(i) *If $\overline{Q}$ is hamiltonian then Q is so.*
(ii) *If Q is hamiltonian and contains at least one idempotent element then $\overline{Q}$ is hamiltonian.*
(iii) *Q is medial iff $\overline{Q}$ is a module.*

Proof. (i) Let $w \in P$, P being a given subquasigroup of Q, and let $(\widetilde{Q}, a)$ be the centrally pointed quasimodule corresponding to the pair (Q, w) in the sense of 8.4. Then P is a subquasimodule of $\widetilde{Q}$ and, since $\widetilde{Q}$ is hamiltonian, P is a block of a congruence r of $\widetilde{Q}$. Now, it is easy to check that r is also a normal congruence of the quasigroup Q.
(ii) Let $e \in Q$ be such that $ee = e$ and let $(\widehat{Q}, a)$ be the centrally pointed quasimodule corresponding to the pointed quasigroup (Q, e). Then $a = ee = e = 0$, and so $e \in P$ for every subquasimodule P of $\widehat{Q}$. Now, P is a normal subquasigroup of Q and the corresponding normal congruence r of Q is also a congruence of the quasimodule $\widehat{Q}$. $\square$

8.7 Lemma. *Let Q be a trimedial quasigroup such that the corresponding quasimodule $\overline{Q}$* (see 8.4, 8.5 and 5.5) *is subdirectly irreducible and nilpotent of class at most 2. Then every non–idempotent subquasigroup P of Q is a normal subquasigroup.*

Proof. Take $w \in P$ such that $a = ww \neq w$ and let $(\overline{Q}, a)$, $\overline{Q} = Q(+, rx)$, be the centrally pointed quasimodule corresponding to (Q, w) in the sense of 8.4. Clearly, $P(+)$ is a subloop of $Q(+)$ and $0 = w \neq a \in V = \mathrm{Z}(Q(+)) \cap P$. Now, V is a non–zero normal subquasimodule of $\overline{Q}$, and hence $\mathrm{A}(Q(+)) \subseteq V$. Thus $\mathrm{A}(Q(+)) \subseteq P$

and P is a normal subquasimodule of $\overline{Q}$. From this it easily follows that P is a normal subquasigroup of Q. $\square$

8.8 Remark. The smallest possible number of elements of a non–medial trimedial quasigroup is 81. According to [7], there exist just 35 isomorphism classes of non–medial trimedial quasigroups of order 81. Now, if Q is such a quasigroup and if Q has no idempotent element then Q is hamiltonian by 8.7.

8.9 Example. Define an operation $\diamondsuit$ on $\mathcal{D}_1$ (see 3.1) by $a\diamondsuit b = (a \bigtriangleup b) + (1,0,0,0)$. Then $\mathcal{D}_1(\diamondsuit)$ is a non-medial CH–quasigroup and $a\diamondsuit a = a + (1,0,0,0) \neq a$ for every $a \in \mathcal{D}_1$. Thus $\mathcal{D}_1(\diamondsuit)$ has no idempotents and is hamiltonian (see 8.7, 8.8).

8.10 Remark. (i) In this remark, let us call a quasigroup Q *meagre* (*minimal*, resp.) if Q is non–trivial and has no proper (non–trivial proper, resp.) subquasigroup.
(ii) Every simple hamiltonian quasigroup is minimal. Conversely, if Q is minimal then Q is hamiltonian and, moreover, if Q contains at least one idempotent then Q is simple.
(iii) Every minimal trimedial quasigroup Q is medial and, moreover, Q is either idempotent or contains just one idempotent element or is meagre.
(iv) Every simple trimedial quasigroup is minimal, finite and medial ([18] and [19]).
(v) Let Q be a finite meagre quasigroup, $|Q| = q$, and P be a finite quasigroup such that $|P| = p$ is prime. Assume further that the product $R = P \times Q$ is a hamiltonian quasigroup and $\mathrm{Hom}(P,Q) = \emptyset$ (e.g., P is meagre and not an image of Q or P is meagre and p does not divide q or P contains no idempotent, Q is simple and not isomorphic to a subquasigroup of P). Then R is not simple and we claim that R is meagre.

Indeed, if S is a subquasigroup of R then $s = |S| \geq q$ (since Q is meagre) and s divides $|R| = qp$ (since R is hamiltonian). If $s > q$ then $s = qp$ (since p is prime) and $S = R$. On the other hand, if $s = q$ then, for every $a \in Q$, there exists a unique $f(a) \in P$ with $(a, f(a)) \in S$. Now, $f : Q \to P$ is a homomorphism, a contradiction.
(vi) Put $R = \mathbb{Z}_5 \times \mathbb{Z}_3$ and define an operation $\circ$ on R by $(a,x) \circ (b,y) = (3a + 3b + 1, 2x + 2y + 1)$. Then $R(\circ)$ is a commutative medial quasigroup and $R(\circ)$ is meagre but not simple (see (iv)).

9. Distributive quasigroups

Recall that a distributive quasigroup is characterized by the equations $x(ab) = (xa)(xb)$ and $(ab)x = (ax)(bx)$ and that every distributive quasigroup is trimedial ([2]). Thus distributive quasigroups are just idempotent trimedial quasigroups.

Put $\mathbf{R}_2 = \mathbb{Z}[\mathbf{x}, \mathbf{x}^{-1}, (1-\mathbf{x})^{-1}]$, $\mathbf{x}$ being an indeterminate over the ring $\mathbb{Z}$ of integers. Then $\mathbf{R}_2$ is a commutative noetherian domain and there exists just one homomorphism $\mathbf{\Phi}$ of $\mathbf{R}_2$ onto $\mathbb{Z}_3$; obviously, we have $\mathbf{\Phi}(\mathbf{x}) = 2$ and $\mathbf{I} = \mathrm{Ker}(\mathbf{\Phi}) = 3\mathbf{R}_2 + (1+\mathbf{x})\mathbf{R}_2$. Further, we denote by $\mathcal{Q}_2$ the variety of $\mathbf{R}_2$–quasimodules and by $\mathcal{D}^p$ the variety of pointed distributive quasigroups.

9.1 Proposition. *The varieties $\mathcal{D}^p$ of pointed distributive quasigroups and $\mathcal{Q}_2$ of $\mathbf{R}_2$–quasimodules are equivalent.*

Proof. Let $(Q, w) \in \mathcal{D}^p$. By 8.2(i), there is an arithmetical form $(Q(+), f, g, 0)$ of Q such that $w = 0$ is the neutral element of $Q(+)$, f, g are 1–central automorphisms of $Q(+)$ and $x = xx = f(x) + g(x)$, $g(x) = (1-f)(x)$ for every $x \in Q$. Consequently,

we may turn $Q(+)$ into a quasimodule $\overline{Q}$ by setting $\mathbf{x}x = f(x)$ (see the proof of 8.4), and so $\lambda(Q, w) = \overline{Q} \in \mathcal{Q}_2$.

Conversely, if $\overline{Q} \in \mathcal{Q}_2$ then $(Q, 0) = \varkappa(\overline{Q})$ is a pointed distributive quasigroup, where the multiplication is defined by $xy = \mathbf{x}x + (1-\mathbf{x})y$ for all $x, y \in Q$.

Now, the correspondences $\lambda : \mathcal{D}^p \to \mathcal{Q}_2$ and $\varkappa : \mathcal{Q}_2 \to \mathcal{D}^p$ represent the desired equivalence between the varieties (again, see the proof of 8.4). □

9.2 Proposition. *Let Q be a distributive quasigroup and let $\overline{Q}$ be the corresponding quasimodule* (see 9.1 and 8.5). *Then:*

(i) *Q is hamiltonian if and only if $\overline{Q}$ is so.*
(ii) *Q is medial iff $\overline{Q}$ is a module.*

Proof. The assertion follows immediately from 8.6. □

9.3 Remark. (i) Let Q be a distributive quasigroup and let $w_1, w_2 \in Q$. Then $w_2 = vw_1$ for some $v \in Q$ and we have $w_2 = \varphi(w_1)$, where $\varphi(x) = vx$ for every $x \in Q$. Clearly, φ is an automorphism of Q, and so φ is also an isomorphism of the pointed quasigroup (Q, w_1) onto the pointed quasigroup (Q, w_2).
(ii) There is a one–to–one correspondence between isomorphism classes of distributive quasigroups and isomorphism classes of $\mathbf{R}_2$–quasimodules. This correspondence preserves the hamiltonian property.

9.4 Remark. Every non–medial distributive quasigroup contains at least 81 elements and there exist just 6 isomorphism classes of non–medial distributive quasigroups of order 81 (see [27]).

9.5 Theorem. *Let A be a ternary $\mathbf{R}_2$–algebra such that $\overline{\tau} \neq 0$ and the underlying module $A' = A(+, rx)$ is cocyclic. Define an operation $\bigtriangledown$ on A by*

$$x \bigtriangledown y = \mathbf{x}x + (1-\mathbf{x})y + (\mathbf{x}^2 + 2\mathbf{x}^3)\tau(x, y, x) + (\mathbf{x} + \mathbf{x}^2 + \mathbf{x}^3)\tau(y, x, y)$$

for all $x, y \in A$. Then $A(\bigtriangledown)$ is a non–medial hamiltonian distributive quasigroup.

Proof. Combine 7.7, 9.1 and 9.2. □

9.6 Remark. (i) A distributive quasigroup Q is simple if and only if Q is non–trivial and contains no non–trivial proper subquasigroup (i.e., Q is minimal).
(ii) Every simple distributive quasigroup is finite and medial.

9.7 Remark. (cf. [11] and [15]) Let P be a minimal subquasigroup of a distributive quasigroup Q.
(i) Let $(Q(+), f, g, 0)$ be an arithmetical form of Q such that $0 \in P$. Then $P(+)$ is a minimal submodule of $Q(+)$ and P is a normal subquasigroup of Q if and only if $P(+)$ is a normal submodule of $Q(+)$ (use 9.1). Now, by 5.11, if P is not normal in Q then $|P| = 3$ and $|Pa \cdot Pb| \in \{3, 9\}$ for all $a, b \in Q$ (according to 2.3, we have $|Pa_0 \cdot Pb_0| = 9$ for some $a_0, b_0 \in Q$). Consequently (see 5.12), P is normal in Q if and only if $|P| \cdot |Pa \cdot Pb| \neq 27$ for all $a, b \in Q$.
(ii) We show that $P \cdot ya = xy \cdot Pa$ for all $x, y \in P$ and $a \in Q$. This is clear for $x = y$ and we assume that $x \neq y$. Put $v = xy \cdot ya$ and $w = x \cdot ya = xy \cdot xa$. Then $v \neq w$, $v, w \in P \cdot ya \cap xy \cdot Pa$ and $|P \cdot ya \cap xy \cdot Pa| \geq 2$. But both $P \cdot ya$ and $xy \cdot Pa$ are minimal subquasigroups of Q and it follows that $P \cdot ya = xy \cdot Pa$.
(iii) It follows easily from (ii) that $P \cdot ya = P \cdot Pa$ for all $y \in P$ and $a \in Q$. In

particular, $|P \cdot Pa| = |P|$ and, since $|p \cdot Pa| = |P|$ and $p \cdot Pa \subseteq P \cdot Pa$, we have $p \cdot Pa = P \cdot Pa$ for every $p \in P$.
(iv) Let $a, b \in Q$ be such that $Pa \cap Pb \neq \emptyset$. We show that then $Pa = Pb$. Indeed, $ua = q = vb$ for some $u, v \in P$ and, by (ii), $P \cdot Pa = P \cdot ua = Pq = P \cdot vb = P \cdot Pb$, $p \cdot Pa = p \cdot Pb$ and, finally, $Pa = Pb$.
(v) According to (iv), $\{Pa \,|\, a \in Q\}$ is a partition of Q.
(vi) ([15, 3.2]) Let $a, b \in Q$ be such that $|Pa \cdot Pb| < |P|^2$. Then $xa \cdot yb = ua \cdot vb$ for some $x, y, u, v \in P$, $(x, y) \neq (u, v)$, $P_1 = Pa$ is a minimal subquasigroup of Q, $P_1 \cdot yb \cap P_1 \cdot vb \neq \emptyset$, and hence $P_1 \cdot yb = P_1 \cdot vb$ by (iv). If $c \in Q$ is such that $yb = xa \cdot c$ then $(pa)(P_1c) = P_1 \cdot P_1c = P_1 \cdot (xa \cdot c) = P_1 \cdot yb = P_1 \cdot vb$ for every $p \in P$ (use (iii)). Now, it is clear that $yb, vb \in Pb \cap P_1c$ and $|Pb \cap P_1c| \geq 2$. Consequently, $Pb = P_1c = Pa \cdot c$ and $Pa \cdot Pb = Pa \cdot (Pa \cdot c) = Pa \cdot (za \cdot c)$ for every $z \in P$ (again, by (iii)). Thus $|Pa \cdot Pb| = |Pa \cdot (za \cdot c)| = |P|$.
(vii) (cf. (i)) We have shown in (vi) that $|Pa \cdot Pb|$ is equal to $|P|$ or $|P|^2$ for all $a, b \in Q$.

9.8 Remark. The variety of pointed commutative distributive quasigroups is equivalent to the variety of $\mathbb{Z}[\frac{1}{2}]$-quasimodules. Since $\mathbb{Z}[\frac{1}{2}]$ is a principal ideal domain, every hamiltonian commutative distributive quasigroup is medial (7.9).

9.9 Remark. (The parastrophes) Let Q be an $\mathbf{R}_2$-quasimodule. Keeping the underlying commutative Moufang loop $Q(+)$ of Q, we introduce three new scalar multiplications, say $\circ$, $*$ and $\bullet$, on Q by the equalities $\mathbf{x} \circ a = (1-\mathbf{x}) \cdot a$, $\mathbf{x} * a = \mathbf{x}^{-1} \cdot a$ and $\mathbf{x} \bullet a = -\mathbf{x}(1-\mathbf{x})^{-1} \cdot a$. Then $(1-\mathbf{x}) \circ a = \mathbf{x} \cdot a$, $(1-\mathbf{x}) * a = (1-\mathbf{x}^{-1}) \cdot a$ and $(1-\mathbf{x}) \bullet a = (1-x)^{-1} \cdot a$ and the resulting quasimodules will be denoted by $\underline{\alpha}(Q) = Q(+, r \circ a)$, $\underline{\beta}(Q) = Q(+, r * a)$ and $\underline{\gamma}(Q) = q(+, r \bullet a)$, respectively (the quasimodule $\underline{\alpha}(Q)$ is called *the opposite quasimodule to* Q and is denoted also by $\overline{Q}$). One may check easily that $\underline{\alpha}^2 = \underline{\beta}^2 = \underline{\gamma}^2 = \mathrm{id}$, $\underline{\alpha}\underline{\beta} = \underline{\gamma}\underline{\alpha} = \underline{\beta}\underline{\gamma}$ and $\underline{\beta}\underline{\alpha} = \underline{\alpha}\underline{\gamma} = \underline{\gamma}\underline{\beta}$ (the six equivalences id, $\underline{\alpha}$, $\underline{\beta}$, $\underline{\gamma}$, $\underline{\alpha}\underline{\beta}$ and $\underline{\beta}\underline{\alpha}$ form a six-element group).

10. Modules of divided powers

Throughout this section, let $\mathbf{S} = \mathbf{R}[\mathbf{x}]$ and $\mathbf{T} = \mathbf{R}[[\mathbf{x}]]$ denote the ring of polynomials and the ring of formal power series in one indeterminate $\mathbf{x}$ over $\mathbf{R}$, respectively. Now, given a (unitary left) $\mathbf{R}$–module M, the direct sum $N = M^{(\omega)} = \{a : \omega \to M \,|\, a(n) = 0$ for almost all $n \in \omega\}$ of ω copies of M becomes a $\mathbf{T}$–module via $(fa)(n) = \sum_{i=0}^{\infty} f_i a(n+i)$ for all $a \in N$ and $f = \sum_{i=0}^{\infty} f_i x^i \in \mathbf{T}$ (the $\mathbf{T}$–module ${}_{\mathbf{T}}N$ is known as the *module of divided powers* and is denoted usually by $M[\mathbf{x}^{-1}]$).

For $n \geq 0$, let $N_n = \{a \in N \,|\, a(m) = 0$ for $m \geq n+1\}$. Clearly, $N_0 \subseteq N_1 \subseteq N_2 \subseteq \dots$ and N_n are submodules of all the three modules ${}_{\mathbf{R}}N$, ${}_{\mathbf{S}}N$ and ${}_{\mathbf{T}}N$.

10.1 Lemma. $\mathbf{S}a = \mathbf{T}a$ *for every* $a \in N$. *If* $a \neq 0$ *then* $\mathbf{S}a \cap N_0 \neq 0$.

Proof. The equality is clear and if $n = \max\{\, i \,|\, a(i) \neq 0\}$ then $0 \neq \mathbf{x}^n a \in N_0$. $\square$

10.2 Lemma. $\mathrm{S}({}_{\mathbf{T}}N) = \mathrm{S}({}_{\mathbf{S}}N) = \mathrm{S}({}_{\mathbf{R}}N_0)$.

Proof. Every submodule of ${}_{\mathbf{R}}N_0$ is also a submodule of ${}_{\mathbf{T}}N$, and hence $\mathrm{S}({}_{\mathbf{R}}N_0) \subseteq \mathrm{S}({}_{\mathbf{T}}N)$. On the other hand, if $\mathbf{T}a$ is a (non–zero) simple submodule of ${}_{\mathbf{T}}N$ then $\mathbf{T}a \cap N_0 \neq 0$, and hence $\mathbf{T}a \subseteq N_0$. Thus $\mathbf{T}a$ is a simple $\mathbf{R}$–module and $\mathbf{T}a \subseteq \mathrm{S}({}_{\mathbf{R}}N_0)$. $\square$

10.3 Lemma. *Let $m \geq 1$. Then* $\mathrm{S}_m({}_{\mathbf{T}}N) = \mathrm{S}_m({}_{\mathbf{S}}N) \subseteq \mathrm{S}_m({}_{\mathbf{R}}N_{m-1}) \subseteq \mathrm{S}_m({}_{\mathbf{R}}N)$ *and* $a \in \mathrm{S}_m({}_{\mathbf{T}}N)$ *if and only if* $a(0) \in \mathrm{S}_m({}_{\mathbf{R}}M)$, $a(1) \in \mathrm{S}_{m-1}({}_{\mathbf{R}}M), \dots, a(m-1) \in \mathrm{S}_1({}_{\mathbf{R}}M)$, $a(m) = a(m+1) = \dots = 0$.

Proof. We shall proceed by induction on m. The case $m = 1$ is settled by 10.2, and so let $m \geq 2$.

First, take $b \in N$ such that ${}_{\mathbf{T}}B = (\mathbf{T}b + P)/P$ is a simple $\mathbf{T}$–module, where $P = \mathrm{S}_{m-1}({}_{\mathbf{T}}N)$. Then ${}_{\mathbf{T}}B \simeq \mathbf{T}/A$ for a maximal ideal A of $\mathbf{T}$ and $\mathbf{x}^k b = 0$ for some $k \geq 1$. Consequently, since $\mathbf{x}^k \in A$ and A is prime, we have $\mathbf{x} \in A$, $\mathbf{x}B = 0$ and $\mathbf{x}b \in P$. Now, by induction, $b(1) \in \mathrm{S}_{m-1}({}_{\mathbf{R}}M), \dots, b(m-1) \in \mathrm{S}_1({}_{\mathbf{R}}M)$, $b(m) = b(m+1) = \dots = 0$. Moreover, since $\mathbf{x}B = 0$ and $P \subseteq \mathrm{S}_{m-1}({}_{\mathbf{R}}N)$, B is also a simple $\mathbf{R}$–module, $(\mathbf{R}b + \mathrm{S}_{m-1}({}_{\mathbf{R}}N))/\mathrm{S}_{m-1}({}_{\mathbf{R}}N)$ is a simple $\mathbf{R}$–module, $b \in \mathrm{S}_m({}_{\mathbf{R}}N)$ and $b(0) \in \mathrm{S}_m({}_{\mathbf{R}}M)$.

Now, conversely, let $a \in N$ be such that $a(i) \in \mathrm{S}_{m-i}({}_{\mathbf{R}}M)$ for $0 \leq i \leq m-1$ and $a(i) = 0$ for $i \geq m$. Then, by induction, $\mathbf{x}a \in P$, and hence $\mathbf{T}a + P = \mathbf{R}a + P$. Moreover, if $C = (\mathbf{R}a + P)/P$ then $xC = 0$ and ${}_{\mathbf{R}}C$ is completely reducible. Consequently, ${}_{\mathbf{T}}C$ is also completely reducible and $a \in \mathrm{S}_m({}_{\mathbf{T}}N)$. $\square$

10.4 Corollary. $\mathrm{S}_\omega({}_{\mathbf{T}}N) = \mathrm{S}_\omega({}_{\mathbf{S}}N) = \mathrm{S}_\omega({}_{\mathbf{R}}N) = \mathrm{S}_\omega({}_{\mathbf{R}}M)^{(\omega)}$. $\square$

10.5 Lemma. *If $m \geq 1$ and* $D_m = \mathrm{S}_m({}_{\mathbf{T}}N)/\mathrm{S}_{m-1}({}_{\mathbf{T}}N)$ *then* $\mathbf{x}D_m = 0$ *and* ${}_{\mathbf{R}}D_m \simeq \mathrm{S}_m({}_{\mathbf{R}}M)/\mathrm{S}_{m-1}({}_{\mathbf{R}}M) \times \mathrm{S}_{m-1}({}_{\mathbf{R}}M)/\mathrm{S}_{m-2}({}_{\mathbf{R}}M) \times \dots \times \mathrm{S}_1({}_{\mathbf{R}}M)/\mathrm{S}_0({}_{\mathbf{R}}M)$.

Proof. The statements follow easily from 10.3. $\square$

10.6 Lemma. *Assume that* $\mathrm{S}_m({}_{\mathbf{R}}M) \neq \mathrm{S}_{m-1}({}_{\mathbf{R}}M)$ *for some $m \geq 1$. Then none of the modules* $\mathrm{S}_m({}_{\mathbf{T}}N)$ *and* $\mathrm{S}_m({}_{\mathbf{S}}N)$ *can be generated by less than m elements.*

Proof. Since $\mathbf{R}$ is noetherian, $\widehat{\mathrm{S}}$–torsion modules have primary decompositions, and hence there is a homogeneous component H of $\mathrm{S}_m({}_{\mathbf{R}}M)$ such that $H = \mathrm{S}_m({}_{\mathbf{R}}H) \neq \mathrm{S}_{m-1}({}_{\mathbf{R}}H)$. From this it follows that $\mathrm{S}_{m-1}({}_{\mathbf{R}}H) \neq \mathrm{S}_{m-2}({}_{\mathbf{R}}H), \dots, \mathrm{S}_1({}_{\mathbf{R}}H) \neq \mathrm{S}_0({}_{\mathbf{R}}H) = 0$ and consequently the module ${}_{\mathbf{R}}D_m$ (see 10.5) contains a copy of $G^{(m)}$ for a simple module G. The direct sum $G^{(m)}$ cannot be generated by $m-1$ elements and, since it is a direct summand of ${}_{\mathbf{R}}D_m$, the same is true for the latter module. $\square$

10.7 Lemma. *If ${}_{\mathbf{R}}M$ is cocyclic then both ${}_{\mathbf{T}}N$ and ${}_{\mathbf{S}}N$ are cocyclic. Moreover, the modules ${}_{\mathbf{R}}M$, ${}_{\mathbf{T}}N$ and ${}_{\mathbf{S}}N$ are artinian and* S_ω*–torsion.*

Proof. See 10.1, [44], Theorem 4.30 and [14], Lemma 6.21. $\square$

10.8 Lemma. ([16], Proposition II.2) *The following conditions are equivalent:*

(i) *${}_{\mathbf{R}}M$ is an injective module.*
(ii) *${}_{\mathbf{T}}N$ is an injective module.*
(iii) *${}_{\mathbf{S}}N$ is an injective module.*

Proof. (i) $\Rightarrow$ (ii). This implication is [30], Theorem 1.
(ii) $\Rightarrow$ (iii). We will use a few standard and well known arguments. First, since $\mathbf{T}$ is the completion of $\mathbf{S}$ in the usual $\mathbf{x}$–adic filtration, the module ${}_{\mathbf{S}}T$ is flat (see e.g. [36], Theorem 8.8). Now, we have the following natural transformation (see [1], Proposition 20.6):

$$\mathrm{Hom}_{\mathbf{S}}({}_{\mathbf{S}}A, {}_{\mathbf{S}}N) \simeq \mathrm{Hom}_{\mathbf{S}}({}_{\mathbf{S}}A, \mathrm{Hom}_{\mathbf{T}}({}_{\mathbf{T}}\mathbf{T}, {}_{\mathbf{T}}N)) \simeq \mathrm{Hom}_{\mathbf{T}}({}_{\mathbf{S}}T \otimes_{\mathbf{S}} A, {}_{\mathbf{T}}N)$$

for every $\mathbf{S}$–module A. Since ${}_{\mathbf{T}}N$ is injective, the functor $\mathrm{Hom}_{\mathbf{T}}({}_{\mathbf{S}}\mathbf{T} \otimes_{\mathbf{S}} -, {}_{\mathbf{T}}N)$ is exact, and hence the same is true for $\mathrm{Hom}_{\mathbf{S}}(-, {}_{\mathbf{S}}N)$. Thus ${}_{\mathbf{S}}N$ is injective.
(iii) $\Rightarrow$ (i). We may proceed in the same way as in the proof of [30], Prop. 1. □

10.9 Let I be a maximal ideal of $\mathbf{R}$ and E be an injective envelope of the simple module $A = \mathbf{R}/I$. Then $K = \mathbf{S}x + \mathbf{S}I$ is a maximal ideal of $\mathbf{S} = \mathbf{R}[\mathbf{x}]$ and $B = \mathbf{S}/K$ is a simple $\mathbf{S}$–module. Now, it follows from 10.7 and 10.8 that the $\mathbf{S}$–module $N = E[\mathbf{x}^{-1}]$ is an injective envelope of (a copy of) ${}_{\mathbf{S}}B$. The module ${}_{\mathbf{S}}N$ is artinian, S_ω–torsion and homogeneous, and every cocyclic $\mathbf{S}$–module containing ${}_{\mathbf{S}}B$ (as the essential simple socle) is isomorphic to a submodule of ${}_{\mathbf{S}}N$. For every $m \geq 1$, $\mathrm{S}_m({}_{\mathbf{S}}N)$ is a module of finite length (i.e., both artinian and noetherian) and if $\mathrm{S}_m({}_{\mathbf{R}}E) \neq \mathrm{S}_{m-1}({}_{\mathbf{R}}E)$ (i.e., if $E \neq \mathrm{S}_{m-1}({}_{\mathbf{R}}E)$) then $\mathrm{S}_m({}_{\mathbf{S}}N)$ cannot be generated by $m-1$ elements (use 10.6).

10.10 Consider the situation from 10.9, take $r_1 \in \mathbf{R}$ and put $K_1 = \mathbf{S}(\mathbf{x} + r_1) + \mathbf{S}I$ and $B_1 = \mathbf{S}/K_1$. Clearly, K_1 is a maximal ideal of $\mathbf{S}$ and B_1 is a simple $\mathbf{S}$–module. Now, denote by $\mathcal{B}$ and $\mathcal{B}_1$ the classes of cocyclic $\mathbf{S}$–modules C and C_1, respectively, such that $\mathrm{S}(C) \simeq B$ and $\mathrm{S}(C_1) \simeq B_1$. If $C \in \mathcal{B}$ then $\Lambda(C) = C_1 \in \mathcal{B}_1$, where both $\mathbf{S}$–modules C and C_1 have the same underlying additive group and the $\mathbf{S}$–scalar multiplication $\cdot$ is defined on C_1 by $r \cdot u = ru$ and $\mathbf{x} \cdot u = \mathbf{x}u - r_1 u$ for all $r \in \mathbf{R}$ and $u \in C$. Moreover, $\Lambda : \mathcal{B} \to \mathcal{B}_1$ is a bijective correspondence and a subset H of C is a submodule of C if and only if it is a submodule of C_1. In particular, the $\mathbf{S}$–modules C and C_1 possess the same number of generators. Finally, a mapping $\varphi : C \to D$ is an $\mathbf{S}$–module homomorphism if and only if $\varphi : \Lambda(C) \to \Lambda(D)$ is an $\mathbf{S}$–module homomorphism (it follows that Λ is a category equivalence).

10.11 Let C be a finite cocyclic $\mathbf{S}$–module such that $\mathbf{x}\mathrm{S}(C) \neq 0$. Then the mapping $u \mapsto \mathbf{x}u$ is an automorphism of C, and hence C becomes a (cocyclic) $\mathbf{R}[\mathbf{x}, \mathbf{x}^{-1}]$–module. Similarly, if $\mathbf{x}v \neq v$ for at least one $v \in \mathrm{S}(C)$, the mapping $u \mapsto (\mathbf{x}-1)u$ is an automorphism of C and C is also an $\mathbf{R}[\mathbf{x}, (\mathbf{x}-1)^{-1}]$–module. Finally, if $\mathbf{x}w \neq 0$ and $\mathbf{x}v \neq v$ for some $v, w \in \mathrm{S}(C)$ then C is an $\mathbf{R}[\mathbf{x}, \mathbf{x}^{-1}, (1-\mathbf{x})^{-1}]$–module.

11. The socle series of $\mathbb{Z}_{p^\infty}[\mathbf{x}^{-1}]$

This section is an immediate continuation of the preceding one. Here, we choose $\mathbf{R} = \mathbb{Z}$, the ring of integers, and $\mathbf{S} = \mathbb{Z}[\mathbf{x}]$, the ring of polynomials with integral coefficients. For a prime number $p \geq 2$, the module $N = \mathbb{Z}_{p^\infty}[\mathbf{x}^{-1}]$ of divided powers is an injective envelope of the simple $\mathbf{S}$–module $B = \mathbf{S}/(\mathbf{S}\mathbf{x} + \mathbf{S}p)$ (see 10.9) and ${}_{\mathbf{S}}N$ is both artinian and S_ω–torsion. Moreover, since $\mathrm{S}_m({}_{\mathbf{S}}N) \neq \mathrm{S}_{m-1}({}_{\mathbf{S}}N)$ for every $m \geq 1$, the m–th member $\mathrm{S}_m({}_{\mathbf{S}}N)$ of the socle series of ${}_{\mathbf{S}}N$ cannot be generated by $m-1$ elements; notice that $|\mathrm{S}_m({}_{\mathbf{S}}N)| = p^{(m+1)m/2}$. Further, it is easy to see that $\mathrm{S}_m({}_{\mathbf{S}}N)$ is isomorphic to the following $\mathbf{S}$–module P_m: $P_m = \mathbb{Z}_{p^m} \times \mathbb{Z}_{p^{m-1}} \times \cdots \times \mathbb{Z}_p$ and $(\mathbf{x}a)(n) = pa(n+1)$ for $0 \leq n \leq m-2$, $(\mathbf{x}a)(m-1) = 0$, $a = (a(0), \ldots, a(m-1)) \in P_m$. Clearly, the additive group $P_m(+)$ (and hence also the module ${}_{\mathbf{S}}P_m$) is generated by the elements $(1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ and $P_1 \simeq \mathrm{S}/(\mathrm{S}3 + \mathrm{S}\mathbf{x})$..

11.1 Lemma. $\mathrm{J}(\mathrm{S}_m({}_{\mathbf{S}}N)) = \mathrm{S}_{m-1}({}_{\mathbf{S}}N) = p\mathrm{S}_m({}_{\mathbf{S}}N)$.

Proof. The factor $\mathrm{S}_m({}_{\mathbf{S}}N)/\mathrm{S}_{m-1}({}_{\mathbf{S}}N)$ is a completely reducible module isomorphic to $P_1^{(m)}$; clearly, $\mathrm{J}(\mathrm{S}_m({}_{\mathbf{S}}N)) \subseteq \mathrm{S}_{m-1}({}_{\mathbf{S}}N)$. On the other hand, $\mathrm{S}_m({}_{\mathbf{S}}N)/\mathrm{J}(\mathrm{S}_m({}_{\mathbf{S}}N))$

is an m–generated completely reducible module, and hence it is also isomorphic to $P_1^{(m)}$. Thus $\mathrm{J}(\mathrm{S}_m({}_{\mathbf{S}}N)) = \mathrm{S}_{m-1}({}_{\mathbf{S}}N)$. $\square$

11.2 Lemma. *The* $\mathbf{S}$*–module* $\mathrm{S}_m({}_{\mathbf{S}}N)$ *is generated by* m *elements but not by* $m-1$ *elements. Every proper submodule of* $\mathrm{S}_m({}_{\mathbf{S}}N)$ *is generated by at most* $m-1$ *elements.*

Proof. Let Q be a proper submodule of P_m. Assume first that $Q + V = P_m$, where $V = \{a(0), 0, \dots, 0)\} \subseteq P_m$. Now, for every i, $1 \le i \le m-1$, there is $a_i(0) \in \mathbb{Z}_{p^m}$ such that $a_1 = (a_1(0), 1, 0, \dots, 0)$, $a_2 = (a_2(0), 0, 1, 0, \dots, 0)$, $\dots$, $a_{m-1} = (a_{m-1}(0), 0, \dots, 0, 1)$ are all in Q. Clearly, $pV \subseteq Q_1 \subseteq Q$, where Q_1 is the submodule generated by the $m-1$ elements $a_1, \dots, a_{m-1}$. We claim that $Q_1 = Q$. Indeed, if $a \in Q$ then $a - b = c \in V$ for some $b \in Q_1$. If $c \notin pV$ then $V = \mathbf{S}c \subseteq Q$ and $Q = P_m$, a contradiction. Thus $c \in pV \subseteq Q_1$ and $a \in Q_1$.

Now, assume that $Q + V \ne P_m$. Then $P = Q/Q \cap V \simeq Q + V/V \subseteq P_m/V \simeq P_{m-1}$, P is isomorphic to a proper submodule of P_{m-1} and, using induction, we conclude that P is generated by at most $m-2$ elements. Finally, since every submodule of V is cyclic, Q is generated by at most $m-1$ elements. $\square$

11.3 Proposition. *Let* Q *be a cocyclic* $\mathbf{S}$*–module whose (essential simple) socle is a copy of* P_1 *(i.e.,* $\mathbb{Z}_p$*, where* $\mathbf{x}\mathbb{Z}_p = 0$*) such that* $\mathrm{S}_m(Q) = Q$*. Then* Q *is isomorphic to a submodule of* $\mathrm{S}_m({}_{\mathbf{S}}N)$ *and* Q *can be generated by at most* m *elements. Moreover, if* Q *cannot be generated by* $m-1$ *elements then* $Q \simeq \mathrm{S}_m({}_{\mathbf{S}}N)$ $(\simeq P_m)$*.*

Proof. Since Q is cocyclic and contains a copy of P_1, Q is isomorphic to a submodule of ${}_{\mathbf{S}}N$. Further, since $\mathrm{S}_m(Q) = Q$, a copy of Q is contained in $\mathrm{S}_m({}_{\mathbf{S}}N)$ and the rest follows from 11.2. $\square$

11.4 Lemma. *Let* Q *be a finitely generated cocyclic* $\mathbf{S}$*–module with* $\mathrm{S}(Q) \simeq P_1$ *and let* $k = \mathrm{gen}(Q)$*. Then:*

(i) *If* $k = 1$ *then* $|Q| \ge p$*, and if* $|Q| = p$ *then* $Q \simeq \mathrm{S}_1({}_{\mathbf{S}}N) \simeq P_1$*.*
(ii) *If* $k = 2$ *then* $|Q| \ge p^3$*, and if* $|Q| = p^3$ *then* $Q \simeq \mathrm{S}_2({}_{\mathbf{S}}N) \simeq P_2$*.*
(iii) *If* $k = 3$ *then* $|Q| \ge p^6$*, and if* $|Q| = p^6$ *and* Q *is not isomorphic to* $\mathrm{S}_3({}_{\mathbf{S}}N)$ *then the* S*–length of* Q *is 4.*
(iv) *If* $k \ge 4$ *then* $|Q| \ge p^7$*.*

Proof. Easy (use 11.3; (iv) follows from (iii), since Q contains a submodule Q_1 with $\mathrm{gen}(Q_1) = 3$). $\square$

11.5 Lemma. $\mathrm{S}_1(P_4)$ *is the set of all* $a \in P_4$ *such that* $a(1) = a(2) = a(3) = 0$ *and* p^3 *divides* $a(0)$*,* $\mathrm{S}_2(P_4)$ *is the set of all* $a \in P_4$ *such that* $a(2) = a(3) = 0$ *and* p^2 *divides* $a(0), a(1)$*, and* $\mathrm{S}_3(P_4)$ *is the set of all* $a \in P_4$ *such that* $a(3) = 0$ *and* p *divides* $a(0), a(1), a(2)$*.*

Proof. Easy. $\square$

11.6 Lemma. *Let* $u, v \in \mathrm{S}_3(P_4)$ *be any elements such that the submodule* $Q = (\mathbf{S}u + \mathbf{S}v + \mathrm{S}(P_4))/\mathrm{S}(P_4)$ *of* $P_4/\mathrm{S}(P_4)$ *is not cyclic. Then* $\mathrm{S}(Q) = \mathrm{S}_1(P_4/\mathrm{S}(P_4)) = \mathrm{S}_2(P_4)/\mathrm{S}_1(P_4) \simeq \mathbb{Z}_p^2$ *is not cyclic.*

Proof. By 11.5, we have $u = (i_0 p, i_1 p, i_2 p, 0)$ and $v = (j_0 p, j_1 p, j_2 p, 0)$, where $0 \le i_0, j_0 \le p^3 - 1$, $0 \le i_1, j_1 \le p^2 - 1$ and $0 \le i_2, j_2 \le p - 1$. If at least one of the elements $u, v, u - v$ is in $\mathrm{S}_2(P_4)$ then $|\mathrm{S}(Q)| = p^2$ (use the fact that Q is not cyclic), and

hence we may assume that none of these elements is in $\mathrm{S}_2(P_4)$ (see 11.5). Further, if $i_1 \neq 0 \neq i_2$ then $(p^2,0,0,0) \in \mathbf{S}u$, $(0,p^2,0,0) \in \mathbf{S}u$ and $\mathrm{S}_2(P_4) \subseteq \mathbf{S}u$. Thus we may also assume that $i_2 = 0$ implies $i_1 = 0$ and, similarly, $j_2 = 0$ implies $j_1 = 0$. On the other hand, if $i_1 = i_2 = j_1 = j_2 = 0$ then $\mathbf{S}u + \mathbf{S}v$ is a cyclic module, a contradiction. Consequently, considering the equalities $\mathbf{S}u + \mathbf{S}(u-v) = \mathbf{S}u + \mathbf{S}v = \mathbf{S}v + \mathbf{S}(u-v)$, we may finally assume that $i_2 = 1$ and $j_1 = j_2 = 0$. Then $(p^2,0,0,0) \in \mathbf{S}u + \mathbf{S}v$, $(0,p^2,0,0) \in \mathbf{S}u + \mathbf{S}v$ and $\mathrm{S}_2(P_4) \subseteq \mathbf{S}u + \mathbf{S}v$. □

11.7 Lemma. *P_2 is not isomorphic to any submodule of $P_4/\mathrm{S}_1(P_4)$.*

Proof. The result follows easily from 11.6. □

11.8 Lemma. *Define an $\mathbf{S}$–module structure on $V = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$ by $\mathbf{x}a = (pa(1), pa(2)), 0)$. Then P_2 is not isomorphic to any submodule of ${}_{\mathbf{S}}V$.*

Proof. Let $u, v \in V$ be such that none of the elements $u, v, u-v$ is in $\mathrm{S}(V)$ and $|\mathrm{S}(\mathbf{S}u)| = p = |\mathrm{S}(\mathbf{S}v)|$. Put $Q = \mathbf{S}u + \mathbf{S}v$. One may check easily that either $|\mathrm{S}(Q)| = p^2$ or Q is cyclic. □

11.9 Lemma. *P_2 is not isomorphic to any submodule of $P_4/\mathrm{S}_2(P_4)$.*

Proof. We have $P_4/\mathrm{S}_2(P_4) \simeq W = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p$, where the $\mathbf{S}$–module structure is given by $\mathbf{x}a = (pa(1), pa(2), pa(3), 0)$. Now, let Q be a submodule of W such that $Q \simeq P_2$. If $A = \{a \mid a(1) = a(2) = a(3) = 0\}$ then $W/A \simeq V$ (see 11.8), and consequently $Q \cap A \neq 0$. In particular, $\mathrm{S}(Q) = \mathbf{S}(p,0,0,0)$. Finally, let $u, v \in Q$ be such that $Q = \mathbf{S}u + \mathbf{S}v$. Then, using the fact that Q is not cyclic, we conclude easily that none of $u, v, u-v$ is in $\mathrm{S}(W)$ and $|\mathrm{S}(Q)| > p$, a contradiction. □

11.10 Proposition. *Let Q be a cocyclic $\mathbf{S}$–module with $\mathrm{S}(Q) \simeq P_1$ and $|Q| = p^6$. Then Q is generated by at most three elements, and if $\mathrm{gen}(Q) = 3$ then $Q \simeq P_3 \simeq \mathrm{S}_3({}_{\mathbf{S}}N)$.*

Proof. Let m denote the S-length of Q. If $m \geq 2$ then (see 11.3) Q is isomorphic to a submodule of $\mathrm{S}_2({}_{\mathbf{S}}N)$ ($\simeq P_2$), and hence $|Q| \leq p^3$, a contradiction. Consequently, $m \geq 3$. Further, if $|\mathrm{J}(Q)| \leq p^2$ then $\mathrm{J}(Q) \subseteq \mathrm{S}_2(Q)$, $Q/\mathrm{S}_2(Q)$ is completely reducible, $m = 3$ and $\mathrm{gen}(Q) \leq 3$ by 11.3 (a contradiction with $|Q/\mathrm{J}(Q)| \geq p^4$). On the other hand, if $|\mathrm{J}(Q)| \geq p^3$ then $|Q/\mathrm{J}(Q)| \leq p^3$ and $\mathrm{gen}(Q) = \mathrm{gen}(Q/\mathrm{J}(Q)) \leq 3$. We have proved that $\mathrm{gen}(Q) \leq 3$. Now, assume that Q is not generated by two elements and that Q is not isomorphic to P_3. By 11.4(iii), $m = 4$, and hence, by 11.3, Q is isomorphic to a submodule of P_4; denote this submodule by Q again and put $Q_1 = Q/\mathrm{S}(P_4)$. Then $|Q_1| = p^5$, the S–length of Q_1 is 3 and, since $\mathrm{S}(P_4) \subseteq \mathrm{J}(Q)$, the module Q_1 cannot be generated by 2 elements. Now, it follows from 11.3 that Q_1 is not cocyclic, and therefore $|\mathrm{S}(Q_1)| \geq p^2$. On the other hand, $\mathrm{S}(Q_1) \subseteq \mathrm{S}(P_4/\mathrm{S}(P_4)) = \mathrm{S}_2(P_4)/\mathrm{S}_1(P_4) \simeq P_1^{(2)}$ and we see that $|\mathrm{S}(Q_1)| = p^2$ and $|Q_1/\mathrm{S}(Q_1)| = p^3$. Further, $Q_1/\mathrm{J}(Q_1)$ is a completely reducible module which is 3–generated but not 2–generated, $Q_1/\mathrm{J}(Q_1) \simeq P_1^{(3)}$, $|Q_1/\mathrm{J}(Q_1)| = p^3$ and $|\mathrm{J}(Q_1)| = p^2$. If $\mathrm{S}(Q_1) \subseteq \mathrm{J}(Q_1)$ then $\mathrm{S}(Q_1) = \mathrm{J}(Q_1)$, a contradiction with the fact that the S–length of $Q_1/\mathrm{S}(Q_1)$ is 2. Consequently, $\mathrm{S}(Q_1) \nsubseteq \mathrm{J}(Q_1)$ and it follows that $Q_1 = A \oplus Q_2$, where A, Q_2 are submodules of Q_1 and A is simple. Since $\mathrm{S}(Q) \simeq P_1$, Q_2 is a cocyclic module and $|Q_2| = p^4$. Clearly, Q_2 is 2–generated and not cyclic. The S–length of Q_2 is 3, and hence either $|\mathrm{S}_2(Q_2)| = p^3$ or $|\mathrm{S}_2(Q_2)| = p^2$. If $|\mathrm{S}_2(Q_2)| = p^3$ then $\mathrm{S}_2(Q_2)$ is a 2–generated cocyclic module of S–length 2 and $\mathrm{S}_2(Q_2) \simeq P_2$ by 11.3. However this is a contradiction with 11.7, and so $|\mathrm{S}_2(Q_2)| =$

p^2 and $\mathrm{S}_2(Q_2) = \mathrm{J}(Q_2)$. Now, $Q_2/\mathrm{S}(Q_2) \simeq P_2$ is isomorphic to a submodule of $P_4/\mathrm{S}_2(P_4)$, which is, finally, a contradiction with 11.9. $\square$

Define another scalar $\mathbf{S}$–multiplication on P_m by $(\mathbf{x} \cdot a)(n) = pa(n+1) - a(n)$ for $0 \le n \le m-2$, $(\mathbf{x} \cdot a)(m-1) = -a(m-1)$, $a = (a(0), \dots, a(m-1)) \in P_m$ (i.e., $\mathbf{x} \cdot a = \mathbf{x}a - a = (\mathbf{x} - 1)a$). In this way (see 10.10), we get a cocyclic $\mathbf{S}$–module $P_{m,1}$, $S(P_{m,1}) \simeq P_{1,1} \simeq \mathbf{S}/(\mathbf{S}p + \mathbf{S}(\mathbf{x}+1))$.

11.11 Proposition. *Let Q_1 be a finitely generated cocyclic $\mathbf{S}$–module such that $\mathrm{S}(Q_1) \simeq P_{1,1}$ and $k = \mathrm{gen}(Q_1)$. Then:*

(i) *If $k \ge 3$ then $|Q_1| \ge p^6$.*
(ii) *If $k \ge 4$ then $|Q_1| \ge p^7$.*

Proof. Combine 11.4 and 10.10. $\square$

11.12 Proposition. *Let Q_1 be a cocyclic $\mathbf{S}$–module with $\mathrm{S}(Q_1) \simeq P_{1,1}$ and $|Q_1| = p^6$. Then Q_1 is generated by at most three elements, and if $\mathrm{gen}(Q_1) = 3$ then $Q_1 \simeq P_{3,1}$.*

Proof. Combine 11.10 and 10.10. $\square$

11.13 Remark. The transformation $a \to \mathbf{x} \cdot a$ is an automorphism of $P_{m,1}(+)$ $(= P_m(+))$, and if $p \ne 2$ then the same is true for the transformation $a \to (\mathbf{x}-1) \cdot a$. Consequently, for $p \ne 2$, the scalar $\mathbf{S}$–multiplication on $P_{m,1}$ can be extended in a unique way to a scalar $\mathbf{R}_2$–multiplication (recall that $\mathbf{R}_2 = \mathbb{Z}[\mathbf{x}, \mathbf{x}^{-1}, (1-\mathbf{x})^{-1}]$) and the cocyclic $\mathbf{S}$–module $P_{m,1}$ turns into a cocyclic $\mathbf{R}_2$–module $P'_{m,1}$ (see 10.11). Notice that $P'_1 \simeq \mathbf{R}_2/(\mathbf{R}_2 p + \mathbf{R}_2(1+\mathbf{x}))$.

11.14 Proposition. *Let $p \ne 2$ and let Q'_1 be a finitely generated cocyclic $\mathbf{R}_2$–module with $S(Q'_1) \simeq P'_{1,1}$ and $k = \mathrm{gen}(Q'_1)$. Then:*

(i) *If $k \ge 3$ then $|Q'_1| \ge p^6$.*
(ii) *If $k \ge 4$ then $|Q'_1| \ge p^7$.*

Proof. Combine 11.11 and 11.13. $\square$

11.15 Proposition. *Let $p \ne 2$ and let Q'_1 be a cocyclic $\mathbf{R}_2$–module with $S(Q'_1) \simeq P'_{1,1}$ and $|Q'_1| = p^6$. Then Q'_1 is generated by at most three elements, and if $\mathrm{gen}(Q'_1) = 3$ then $Q'_1 \simeq P'_{3,1}$.*

Proof. Combine 11.12, 11.13 and use the fact that $\mathbf{x}^{-1} \cdot a = \mathbf{x}^k \cdot a$ and $(1-\mathbf{x})^{-1} \cdot a = (1-\mathbf{x})^l \cdot a$ for some positive integers k and l. $\square$

12. The synthesis

12.1 In this (final) section, let $p = 3$ and let $\mathcal{P}$ ($\mathcal{C}$, resp.) denote the simple (cocyclic, resp.) $\mathbf{R}_2$–module $P'_{1,1}$ ($P'_{3,1}$, resp.) defined in the preceding section. Recall that $\mathcal{P}(+) = \mathbb{Z}_3(+)$, $|\mathcal{P}| = 3^1 = 3$, $3a = (1+\mathbf{x}) \cdot a = 0$ and $\mathbf{x} \cdot a = \mathbf{x}^{-1} \cdot a = (1-\mathbf{x}) \cdot a = (1-\mathbf{x})^{-1} \cdot a = -a$ for every $a \in \mathcal{P}$. Further, $\mathcal{C}(+) = \mathbb{Z}_{27}(+) \times \mathbb{Z}_9(+) \times \mathbb{Z}_3(+)$, $|\mathcal{C}| = 3^6 = 729$, $3a = (3a(0), 3a(1), 0)$, $(1+\mathbf{x}) \cdot a = (3a(1), 3a(2), 0)$, $\mathbf{x} \cdot a = (26a(0) + 3a(1), 8a(1) + 3a(2), 2a(2))$, $\mathbf{x}^{-1} \cdot a = \mathbf{x}^{17} \cdot a = (26a(0) + 24a(1) + 18a(2), 8a(1) + 6a(2), 2a(2))$, $(1-\mathbf{x}) \cdot a = (2a(0) + 24a(1), 2a(1) + 6a(2), 2a(2))$ and $(1-\mathbf{x})^{-1} \cdot a = (1-\mathbf{x})^{17} \cdot a = (14a(0) + 21a(1) + 18a(2), 5a(1) + 3a(2), 2a(2))$ for every $a = (a(0(, a(1), a(2)) \in \mathcal{C}$ (the transformations $a \to \mathbf{x} \cdot a$ and $a \to (1-\mathbf{x}) \cdot a$ are

permutations of $\mathcal{C}$ and both have order 18 in the corresponding symmetric group). We have $\mathrm{S}(\mathcal{C}) \simeq \mathcal{P}$, $\mathrm{gen}(\mathcal{C}) = 3$ and, of course, $\mathcal{C}$ is $\widehat{K}$–torsion. By 11.15, $C \simeq \mathcal{C}$ whenever C is a cocyclic $\mathbf{R}_2$–module with $\mathrm{S}(C) \simeq \mathcal{P}$, $\mathrm{gen}(C) = 3$ and $|C| = 729$. We put $\mathbf{u} = (1,0,0)$, $\mathbf{v} = (0,1,0)$ and $\mathbf{w} = (0,0,1)$, $\mathbf{u},\mathbf{v},\mathbf{w} \in \mathcal{C}$. Notice also that the mapping $\lambda : a \mapsto (a(0), a(0)+8a(1), a(0)+a(1)+a(2))$ is an automorphism of $\mathcal{C}(+)$ such that $\lambda^2 = \mathrm{id}$, $\lambda(\mathbf{x}\cdot a) = (1-\mathbf{x})\cdot\lambda(a)$ and $\lambda((1-\mathbf{x})\cdot a) = \mathbf{x}\cdot\lambda(a)$. Similarly, the mapping $\varkappa : a \mapsto (a(0), -a(1)+6a(2), a(2))$ is an automorphism of $\mathcal{C}(+)$ such that $\varkappa(\mathbf{x}\cdot a) = \mathbf{x}^{-1}\cdot\varkappa(a)$, $\varkappa((1-\mathbf{x})\cdot a) = (1-\mathbf{x}^{-1})\cdot\varkappa(a)$ and the mapping $\mu : a \mapsto (a(0)+9a(1), a(0)+a(1)+3a(2), a(0)+2a(1)+a(2))$ is an automorphism of $\mathcal{C}(+)$ such that $\mu(\mathbf{x}\cdot a) = (1-\mathbf{x})^{-1}\cdot\mu(a)$ and $\mu((1-\mathbf{x})\cdot a) = -\mathbf{x}(1-\mathbf{x})^{-1}\cdot\mu(a)$. Finally, $\mu\lambda$ is an automorphism of $\mathcal{C}(+)$ such that $\mu\lambda(\mathbf{x}\cdot a) = -\mathbf{x}(1-\mathbf{x})^{-1}\cdot\mu\lambda(a)$ and $\mu\lambda((1-\mathbf{x})\cdot a) = (1-\mathbf{x})^{-1}\cdot\mu\lambda(a)$.

12.2 Let us define $\tau_1(a,b,c) = (9a(0)b(1)c(2)+18a(1)b(0)c(2),0,0)$ and $\tau_2(a,b,c) = (18a(0)b(1)c(2)+9a(1)b(0)c(2),0,0)$ for all $a,b,c \in \mathcal{C}$ (see 12.1). One checks readily that τ_1, τ_2 are trilinear mappings of $\mathcal{C}^{(3)}$ into $\mathcal{C}$ and that these mappings satisfy the four conditions T(0), … ,T(3) from 1.5. Moreover, $\tau_2 = -\tau_1 = 26\tau_1$, $\overline{\tau_1}(a,b,c) = (9a(0)b(1)c(2)+9a(1)b(2)c(0)+9a(2)b(0)c(1)+18a(0)b(2)c(1)+18a(1)b(0)c(2)+18a(2)b(1)c(0),0,0) = -\overline{\tau_2}(a,b,c)$, $\overline{\tau_1}(\mathbf{u},\mathbf{v},\mathbf{w}) = (9,0,0) = 9\mathbf{u}$, $\overline{\tau_2}(\mathbf{u},\mathbf{v},\mathbf{w}) = (18,0,0) = 18\mathbf{u}$. Thus $(\mathcal{C},\tau_1)$ and $(\mathcal{C},\tau_2)$ are ternary algebras (see 1.5) with $\overline{\tau_1} \neq 0 \neq \overline{\tau_2}$.

12.2.1 Define a mapping $\vartheta : \mathcal{C}^{(3)} \mapsto \mathcal{C}$ by $\vartheta(a,b,c) = (9(a(1)b(0)-a(0)b(1))(c(0)+c(1)),0,0)$ for all $a,b,c \in \mathcal{C}$. Clearly, ϑ is a trilinear mapping satisfying T(0), … ,T(3) and $\overline{\vartheta} = 0$. Now, consider the automorphism λ of $\mathcal{C}(+)$ defined in 12.1. The following result is quite easy:

12.2.1.1 Lemma. *$\vartheta(a,b,a-b) = (9(a(1)b(0)-a(0)b(1))(a(0)+a(1)-b(0)-b(1)),0,0) = \tau_1(a,b,a-b)+\tau_1(\lambda(a),\lambda(b),\lambda(a-b))$ for all $a,b \in \mathcal{C}$.* □

12.2.2 Put $\sigma(a) = (18a(0)^3+9a(0)^2a(1)+18a(0)a(1)^2+9a(0),0,0)$ for every $a \in \mathcal{C}$.

12.2.2.1 Lemma. *$\sigma(a)+\sigma(b) = \sigma(a+b)+\vartheta(a,b,a-b)$ for all $a,b \in \mathcal{C}$.*

Proof. Easy to check directly. □

12.2.2.2 Lemma. (i) *$\sigma(a) \neq 0$ if and only if 3 divides $a(0)+a(1)$ and 3 does not divide $a(0)$ (or $a(1)$).*
(ii) *If $\sigma(a) \neq 0$ then $\sigma(a) = 9a$.*

Proof. Use the equality $(a(0)+a(1)+1)(a(0)+a(1)+2)a(0) = a(0)^3+2a(0)^2a(1)+a(0)a(1)^2+2a(0)+3a(0)^2+3a(0)a(1)$. □

12.2.2.3 Corollary. *$\sigma(a) \neq 0$ if and only if either $a \in \{(1,2,0),(1,2,1),(1,2,2)\}+3\mathcal{C}$ (and then $\sigma(a) = (9,0,0)$) or $a \in \{(2,1,0),(2,1,1),(2,1,2)\}+3\mathcal{C}$ (and then $\sigma(a) = (18,0,0)$).* □

12.2.2.4 Corollary. *$|\{a \,|\, \sigma(a) = 0\}| = 567$ and $|\{a \,|\, \sigma(a) \neq 0\}| = 162$.* □

12.2.3 Put $\xi(a) = \lambda(a)+\sigma(a) = (18a(0)^3+9a(0)^2a(1)+18a(0)a(1)^2+10a(0), a(0)+8a(1), a(0)+a(1)+a(2))$ for every $a \in \mathcal{C}$.

12.2.3.1 Lemma. *$\xi^2(a) = a+2\sigma(a)$ for every $a \in \mathcal{C}$.*

Proof. We have $\xi^2(a) = \xi(\lambda(a)+\sigma(a)) = \lambda(\lambda(a)+\sigma(a))+\sigma(\lambda(a)+\sigma(a)) = \lambda^2(a)+\lambda\sigma(a)+\sigma\lambda(a)+\sigma^2(a)-\vartheta(\lambda(a),\sigma(a),\lambda(a)-\sigma(a))$ by 12.2.2.1. On the other

hand, $\lambda^2 = \mathrm{id}$, $\lambda\sigma(a) = \sigma(a) = \sigma\lambda(a)$, $\sigma^2(a) = 0 = \vartheta(\lambda(a), \sigma(a), \lambda(a) - \sigma(a))$, and so $\xi^2(a) = a + 2\sigma(a)$. □

12.2.3.2 Corollary. *$\xi^2(a) = a$ if and only if $\sigma(a) = 0$.* □

12.2.3.3 Lemma. *ξ is a permutation of $\mathcal{C}$.*

Proof. Since $\mathcal{C}$ is finite, it suffices to show that ξ is injective. However, if $\xi(a) = \xi(b)$ then $a + 2\sigma(a) = \xi^2(a) = \xi^2(b) = b + 2\sigma(b)$, and hence $a(1) = b(1)$ and $a(2) = b(2)$. Further, $3a = 3a + 6\sigma(a) = 3b + 6\sigma(b) = 3b$, and so 27 divides $3(a(0) - b(0))$. From this, 27 divides $18(a(0)^3 - b(0)^3)$, etc., and we conclude that $0 = a + 2\sigma(a) - b - 2\sigma(b) = (19(a(0) - b(0)), 0, 0)$. Thus $a(0) = b(0)$ and $a = b$. □

12.2.3.4 Lemma. *$\xi(\mathbf{x} \cdot a) = (1 - \mathbf{x}) \cdot \xi(a)$ and $\xi((1 - \mathbf{x}) \cdot a) = \mathbf{x} \cdot \xi(a)$ for every $a \in \mathcal{C}$.*

Proof. We have $\xi(\mathbf{x}\cdot a) = \lambda(\mathbf{x}\cdot a)+\sigma(\mathbf{x}\cdot a) = (1-\mathbf{x})\cdot\lambda(a)+\sigma(\mathbf{x}\cdot a)$. It is easy to check that $\sigma(\mathbf{x}\cdot a) = -\sigma(a) = (1-\mathbf{x})\cdot\sigma(a)$, and hence $\xi(\mathbf{x}\cdot a) = (1-\mathbf{x})\cdot\lambda(a)+(1-\mathbf{x})\cdot\sigma(a) = (1 - \mathbf{x}) \cdot \xi(a)$. Quite similarly, $\xi((1 - \mathbf{x}) \cdot a) = \mathbf{x} \cdot \xi(a)$. □

12.2.3.5 Lemma. *$\xi(a+b+\tau_1(a, b, a-b)) = \xi(a)+\xi(b)+\tau_2(\xi(a), \xi(b), \xi(a)-\xi(b))$ for all $a, b \in \mathcal{C}$.*

Proof. Using 12.2.1.1 and 12.2.2.1, one checks easily that $\xi(a+b+\tau_1(a, b, a-b)) = \lambda(a) + \lambda(b) + \tau_1(a, b, a-b) + \sigma(a+b) = \xi(a) + \xi(b) + \tau_1(a, b, a-b) - \vartheta(a, b, a-b) = \xi(a)+\xi(b)-\tau_1(\lambda(a), \lambda(b), \lambda(a)-\lambda(b)) = \xi(a)+\xi(b)-\tau_1(\xi(a), \xi(b), \xi(a)-\xi(b))$. □

12.3 Define operations $\circledast$ and $\boxtimes$ on $\mathcal{C}$ (see 12.1, 12.2) by $a\circledast b = a+b+\tau_1(a, b, a-b) = (a(0)+b(0)+9a(0)a(2)b(1)+18a(0)b(1)b(2)+18a(1)a(2)b(0)+9a(1)b(0)b(2), a(1)+b(1), a(2)+b(2))$ and $a \boxtimes b = a + b + \tau_2(a, b, a - b) = (a(0) + b(0) + 18a(0)a(2)b(1) + 9a(0)b(1)b(2) + 9a(1)a(2)b(0) + 18a(1)b(0)b(2), a(1) + b(1), a(2) + b(2))$ for all $a, b \in \mathcal{C}$. By 6.1, $\mathcal{C}(\circledast)$ and $\mathcal{C}(\boxtimes)$ are commutative Moufang loops and it is easy to see that the mapping $(a(0), a(1), a(2)) \to (a(0), a(1), 2a(2))$ is an isomorphism of $\mathcal{C}(\circledast)$ onto $\mathcal{C}(\boxtimes)$. In fact, by [27, 6.3], these (isomorphic) loops are determined by three generators, say α, β, γ, and relations $27\alpha = 9\beta = 3\gamma = 0$, $[\alpha, \beta, \gamma] = 9\alpha$ (or $[\alpha, \beta, \gamma] = 18\alpha$). By 12.2.3.2 and 12.2.3.5, $\xi : \mathcal{C}(\circledast) \mapsto \mathcal{C}(\boxtimes)$ is another isomorphism of the loops. Notice that $\xi(\mathbf{u}) = (1, 1, 1)$, $\xi(\mathbf{v}) = (0, -1, 1)$, $\xi(\mathbf{w}) = (0, 0, 1)$, $[\xi(\mathbf{u}), \xi(\mathbf{v}), \xi(\mathbf{w})]_{\mathcal{C}(\circledast)} = \overline{\tau_1}((1, 1, 1), (0, -1, 1), (0, 0, 1)) = (18, 0, 0) = 18\mathbf{u} = 18\xi(\mathbf{u})$ and $[\xi(\mathbf{u}), \xi(\mathbf{v}), \xi(\mathbf{w})]_{\mathcal{C}(\boxtimes)} = (9, 0, 0) = 9\mathbf{u} = 9\xi(\mathbf{u})$.

12.4 Put $\mathcal{C}'_1 = \mathrm{q}(\mathcal{C}, \tau_1) = \mathcal{C}(\circledast, rx)$ and $\mathcal{C}'_2 = \mathrm{q}(\mathcal{C}, \tau_2) = \mathcal{C}(\boxtimes, rx)$ (see 6.1 and 12.3). By 7.7, both $\mathcal{C}'_1$ and $\mathcal{C}'_2$ are non–associative cocyclic ($\widehat{K}$–torsion) $\mathbf{R}_2$–quasimodules and we have $\mathrm{gen}(\mathcal{C}'_1) = 3 = \mathrm{gen}(\mathcal{C}'_2)$.

12.4.1 Lemma. (i) $27\mathbf{u} = 9\mathbf{v} = 3\mathbf{w} = 0$.
(ii) $(1 + \mathbf{x}) \cdot \mathbf{u} = 0$, $(1 + \mathbf{x}) \cdot \mathbf{v} = 3\mathbf{u}$ *and* $(1 + \mathbf{x}) \cdot \mathbf{w} = 3\mathbf{v}$.
(iii) $[\mathbf{u}, \mathbf{v}, \mathbf{w}]_{\mathcal{C}'_1} = 9\mathbf{u}$ *and* $[\mathbf{u}, \mathbf{v}, \mathbf{w}]_{\mathcal{C}'_2} = 18\mathbf{u}$.

Proof. See 12.1, 12.2 and 12.3. □

12.4.2 Lemma. *The quasimodules $\mathcal{C}'_1$ and $\mathcal{C}'_2$ are not isomorphic.*

Proof. Let, on the contrary, $\varphi : \mathcal{C}'_2 \to \mathcal{C}'_1$ be an isomorphism. Put $u = \varphi(\mathbf{u})$, $v = \varphi(\mathbf{v})$ and $w = \varphi(\mathbf{w})$. We have $(3u(1), 3u(2), 0) = (1 + \mathbf{x}) \cdot u = \varphi((1 + \mathbf{x}) \cdot \mathbf{u}) = 0$, and hence $u(1) = 0 = u(2)$. Similarly, $(3v(1), 3v(2), 0) = (1 + \mathbf{x}) \cdot v =$

$\varphi((1+\mathbf{x})\cdot\mathbf{v}) = \varphi(3\mathbf{u}) = 3u = (3u(0),0,0)$, 9 divides $u(0)-v(1)$, $v(2)=0$, $(3w(1),3w(2),0) = (1+\mathbf{x})\cdot w = \varphi((1+\mathbf{x})\cdot\mathbf{w}) = \varphi(3\mathbf{v}) = 3v = (3v(0),3v(1),0)$, 9 divides $v(0)-w(1)$, 3 divides $v(1)-w(2)$. Furthermore, the orders of u, v and w are 27, 9 and 3, resp., and so 3 does not divide $u(0)$, 3 divides $v(0)$, 3 does not divide $v(1)$, 9 divides $w(0)$, 3 divides $w(1)$ and $w(2)\neq 0$. Finally, $(9u(0)v(1)w(2),0,0) = \overline{\tau_1}(u,v,w) = [u,v,w]_{\mathcal{C}_1'} = \varphi([\mathbf{u},\mathbf{v},\mathbf{w}]_{\mathcal{C}_2'}) = \varphi(18\mathbf{u}) = 18u = (18u(0),0,0)$, hence $9u(0)(2-v(1)w(2)) = 0 \pmod{27}$ and 3 divides $2-v(1)w(2)$. Thus we have shown that 3 divides $2-w(2)^2$, since $2-w(2)^2 = 2-w(1)w(2)+w(1)w(2)-w(2)^2$. But this is a contradiction with $w(2)=1$ or 2. □

12.4.3 Lemma. *The permutation ξ of $\mathcal{C}$* (see 12.2.3) *is an anti–isomorphism of the quasimodule $\mathcal{C}_1'$ onto the quasimodule $\mathcal{C}_2'$.*

Proof. By 12.2.3.4 and 12.2.3.5, we have $\xi(a\circledast b) = \xi(a)\boxtimes\xi(b)$, $\xi(\mathbf{x}\cdot a) = (1-\mathbf{x})\cdot\xi(a)$, $\xi((1-\mathbf{x})\cdot a) = \mathbf{x}\cdot\xi(a)$ for all $a,b\in\mathcal{C}$ and this means that ξ is an anti–isomorphism of the quasimodules. □

12.4.4 Remark. Let $\overline{\mathcal{C}_1'}$ ($\overline{\mathcal{C}_2'}$, resp.) denote the quasimodule opposite to $\mathcal{C}_1'$ ($\mathcal{C}_2'$, resp.). That is, $\mathcal{C}(\circledast)$ ($\mathcal{C}(\boxtimes)$, resp.) is the underlying commutative Moufang loop of $\overline{\mathcal{C}_1'}$ ($\overline{\mathcal{C}_2'}$, resp.) and the (opposite) scalar multiplication, say $\circ$, is given (in both cases) by $\mathbf{x}\circ a = (1-\mathbf{x})\cdot a$ and $(1-\mathbf{x})\circ a = \mathbf{x}\cdot a$. If $\mathbf{u}_1 = (1,1,1)$ and $\mathbf{v}_1 = (0,-1,1)$ then $\overline{\mathcal{C}_1'}$ ($\overline{\mathcal{C}_2'}$, resp.) is generated by $\{\mathbf{u}_1,\mathbf{v}_1,\mathbf{w}\}$, $27\mathbf{u}_1 = 9\mathbf{v}_1 = 3\mathbf{w} = 0$, $(1+\mathbf{x})\circ\mathbf{u}_1 = 0$, $(1+\mathbf{x})\circ\mathbf{v}_1 = 3\mathbf{u}_1$ and $(1+\mathbf{x})\circ\mathbf{w} = 3\mathbf{v}_1$, and $[\mathbf{u}_1,\mathbf{v}_1,\mathbf{w}]_{\mathcal{C}(\circledast)} = 18\mathbf{u}_1$ ($[\mathbf{u}_1,\mathbf{v}_1,\mathbf{w}]_{\mathcal{C}(\boxtimes)} = 9\mathbf{u}_1$, resp.). Now, it follows from 12.5.1 that there exist quasimodule isomorphisms $\zeta_1 : \mathcal{C}_2' \mapsto \overline{\mathcal{C}_1'}$, $\zeta_2 : \mathcal{C}_1' \mapsto \overline{\mathcal{C}_2'}$ such that $\zeta_1(\mathbf{u}) = \mathbf{u}_1 = \zeta_2(\mathbf{u})$, $\zeta_1(\mathbf{v}) = \mathbf{v}_1 = \zeta_2(\mathbf{v})$ and $\zeta_1(\mathbf{w}) = \mathbf{w} = \zeta_2(\mathbf{w})$. Then, of course, ζ_1 is an anti–isomorphism of $\mathcal{C}_2'$ onto $\mathcal{C}_1'$, ζ_2 is an anti–isomorphism of $\mathcal{C}_1'$ onto $\mathcal{C}_2'$ and, in fact, $\zeta_1 = \xi^{-1} = \zeta_2^{-1}$, $\zeta_2 = \xi = \zeta_1^{-1}$ (use 12.2.3.2 and 12.4.3).

12.4.5 Remark. (i) Putting $\mathbf{w}_1 = (0,6,1)$, we have $27\mathbf{u} = 9(-\mathbf{v}) = 3\mathbf{w}_1 = 0$, $(1+\mathbf{x}^{-1})\cdot\mathbf{u} = 0$, $(1+\mathbf{x}^{-1})\cdot(-\mathbf{v}) = 3\mathbf{u}$, $(1+\mathbf{x}^{-1})\cdot\mathbf{w}_1 = -3\mathbf{v}$, $[\mathbf{u},-\mathbf{v},\mathbf{w}_1]_{\mathcal{C}(\circledast)} = 18\mathbf{u}$ and $[\mathbf{u},-\mathbf{v},\mathbf{w}_1]_{\mathcal{C}(\boxtimes)} = 9\mathbf{u}$. Consequently, considering the parastrophes $\underline{\beta}(\mathcal{C}_1')$, $\underline{\beta}(\mathcal{C}_2')$ (see 9.8) and 12.5.1, we get quasimodule isomorphisms $\eta_1 : \mathcal{C}_2' \mapsto \underline{\beta}(\mathcal{C}_1')$ and $\eta_2 : \mathcal{C}_1' \mapsto \underline{\beta}(\mathcal{C}_2')$ such that $\eta_1(\mathbf{u}) = \mathbf{u} = \eta_2(\mathbf{u})$, $\eta_1(\mathbf{v}) = -\mathbf{v} = \eta_2(\mathbf{v})$ and $\eta_1(\mathbf{w}) = \mathbf{w}_1 = \eta_2(\mathbf{w})$. In fact, $\eta_2 = \eta_1^{-1}$.
(ii) Put $\mathbf{u}_2 = (10,5,1)$, $\mathbf{v}_2 = (18,2,2)$ and $\mathbf{w}_2 = (0,3,1)$. Then we have $27\mathbf{u}_2 = 9\mathbf{v}_2 = 3\mathbf{w}_2 = 0$, $(1-2\mathbf{x})(1-\mathbf{x})^{-1}\cdot\mathbf{u}_2 = 0$ $(= (1-2\mathbf{x})\cdot\mathbf{u}_2)$, $(1-\mathbf{x})^{-1}\cdot\mathbf{u}_2 = 2\mathbf{u}_2$, $(1-2\mathbf{x})(1-\mathbf{x})^{-1}\cdot\mathbf{v}_2 = 3\mathbf{u}_2$, $(1-2\mathbf{x})(1-\mathbf{x})^{-1}\cdot\mathbf{w}_2 = 3\mathbf{v}_2$, $[\mathbf{u}_2,\mathbf{v}_2,\mathbf{w}_2]_{\mathcal{C}(\circledast)} = 18\mathbf{u}_2$ and $[\mathbf{u}_2,\mathbf{v}_2,\mathbf{w}_2]_{\mathcal{C}(\boxtimes)} = 9\mathbf{u}_2$. Similarly as in (i), we get quasimodule isomorphisms $\varrho_1 : \mathcal{C}_2' \mapsto \underline{\gamma}(\mathcal{C}_1')$ and $\varrho_2 : \mathcal{C}_1' \mapsto \underline{\gamma}(\mathcal{C}_2')$ such that $\varrho_1(\mathbf{u}) = \mathbf{u}_2 = \varrho_2(\mathbf{u})$, $\varrho_1(\mathbf{v}) = \mathbf{v}_2 = \varrho_2(\mathbf{v})$ and $\varrho_1(\mathbf{w}) = \mathbf{w}_2 = \varrho_2(\mathbf{w})$. Again, $\varrho_2 = \varrho_1^{-1}$.
(iii) According to (i), (ii), 12.4.3, 12.4.4 and 9.9, we have the following quasimodule isomorphisms: $\mathcal{C}_1' \simeq \underline{\alpha}(\mathcal{C}_2') \simeq \underline{\beta}(\mathcal{C}_2') \simeq \underline{\gamma}(\mathcal{C}_2') \simeq \underline{\alpha\beta}(\mathcal{C}_1') \simeq \underline{\beta\alpha}(\mathcal{C}_1') \simeq \underline{\alpha\gamma}(\mathcal{C}_1') \simeq \underline{\gamma\alpha}(\mathcal{C}_1') \simeq \underline{\beta\gamma}(\mathcal{C}_1') \simeq \underline{\gamma\beta}(\mathcal{C}_1')$ and $\mathcal{C}_2' \simeq \underline{\alpha}(\mathcal{C}_1') \simeq \underline{\beta}(\mathcal{C}_1') \simeq \underline{\gamma}(\mathcal{C}_1') \simeq \underline{\alpha\beta}(\mathcal{C}_2') \simeq \underline{\beta\alpha}(\mathcal{C}_2') \simeq \underline{\alpha\gamma}(\mathcal{C}_2') \simeq \underline{\gamma\alpha}(\mathcal{C}_2') \simeq \underline{\beta\gamma}(\mathcal{C}_2') \simeq \underline{\gamma\beta}(\mathcal{C}_2')$.

12.5 Let F be a free $\mathbf{R}_2$–quasimodule freely generated by a three–element set $\{\alpha,\beta,\gamma\}$ (see 6.2). Then F is nilpotent of class at most 2 and we denote by G_1 (G_2, resp.) the subquasimodule generated by the elements 27α, 9β, 3γ, $(1+\mathbf{x})\alpha$, $(1+\mathbf{x})\beta\ominus 3\alpha$, $(1+\mathbf{x})\gamma\ominus 3\beta$ and $[\alpha,\beta,\gamma]\ominus 9\alpha$ ($[\alpha,\beta,\gamma]\ominus 18\alpha$, resp.). Then $G_1\subseteq \mathrm{Z}(F)$ ($G_2\subseteq \mathrm{Z}(F)$, resp.), and hence G_1 (G_2, resp.) is a normal submodule of F.

12.5.1 Lemma. *$F/G_1) \simeq \mathcal{C}_1'$ ($F/G_2 \simeq \mathcal{C}_2'$, resp.).*

Proof. The assertion follows easily from 6.2, but we may also proceed in the following way: First, 12.4.1 implies that $\mathcal{C}_1' \simeq F/H$ for a normal subquasimodule H of F with $G_1 \subseteq H$. If K is the (normal) subquasimodule of F such that $G_1 \subseteq K$ and $K/G_1) = \mathrm{A}(F/G_1)$ then $[\alpha, \beta, \gamma] \in K$, $M = G_1/K$ is a module and if $\pi : F \to M$ is the natural projection then $9\pi(\alpha) = 9\pi(\beta) = 3\pi(\gamma) = 0$, $\mathbf{x}\pi(\alpha) = -\alpha$, $\mathbf{x}\pi(\beta) = 3\alpha - \beta$, $\mathbf{x}\pi(\gamma) = 3\beta - \gamma$. It follows easily that the additive group $M(+)$ is generated by the elements $\pi(\alpha), \pi(\beta), \pi(\gamma)$ and $|M| \leq 3^5 = 243$. On the other hand, $|K/G_1)| = |\mathrm{A}(F/G_1)| = 3$, and therefore $729 \geq |F/G_1| \geq |F/H| = 729$, $G_1 = H$ and $F/G_1 \simeq \mathcal{C}_1'$. $\square$

12.6 Theorem. *Every non–associative cocyclic $\mathbf{R}_2$–quasimodule contains at least 729 elements and the only non–associative cocyclic $\mathbf{R}_2$–quasimodules of order 729 are (up to isomorphism) the non–isomorphic quasimodules $\mathcal{C}_1'$ and $\mathcal{C}_2'$* (see 12.4)*. These two quasimodules are anti–isomorphic.*

Proof. The first assertion follows by easy combination of 7.7 and 11.11. Now, let Q be a non–associative cocyclic $\mathbf{R}_2$–quasimodule of order 729. By 7.7, there exists a ternary algebra A $(= A(+, rx, \tau))$ such that $Q = \mathrm{q}(A)$, $\overline{\tau} \neq 0$, the module $A' = A(+, rx)$ is cocyclic and $\widehat{K}$–torsion, and $\mathrm{gen}(A') \geq 3$. By 11.15, we have $A' \simeq P_{3,1}'$ and we can assume that $A' = P_{3,1}'$ (see 11.13). We have $27\mathbf{u} = 9\mathbf{v} = 3\mathbf{w} = 0$, $(1 + \mathbf{x}) \cdot \mathbf{u} = 0$, $(1 + \mathbf{x}) \cdot \mathbf{v} = 3\mathbf{u}$, $(1 + \mathbf{x}) \cdot \mathbf{w} = 3\mathbf{v}$ and, since Q is cocyclic and $9Q$ is a non–trivial normal subquasimodule of Q, we also have $\mathrm{A}(Q) \subseteq 9Q$ and $[\mathbf{u}, \mathbf{v}, \mathbf{w}] \in \{9\mathbf{u}, 18\mathbf{u}\}$. The subquasimodule P of Q generated by $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ is non–associative and cocyclic, hence $|P| \geq 729$ and necessarily $P = Q$. Now, it follows from 12.5.1 that Q is a homomorphic image of $\mathcal{C}_1'$ or $\mathcal{C}_2'$, and consequently either $Q \simeq \mathcal{C}_1'$ or $Q \simeq \mathcal{C}_2'$. Finally, $\mathcal{C}_1'$ and $\mathcal{C}_2'$ are not isomorphic (12.4.2) but they are anti–isomorphic (12.4.3; see also 12.4.4). $\square$

12.7 Define two binary operations $\bigtriangledown_1$ and $\bigtriangledown_2$ on $\mathcal{C}$ by $a \bigtriangledown_1 b = \mathbf{x} \cdot a \circledast (1 - \mathbf{x}) \cdot b = (26a(0) + 3a(1), 8a(1) + 3a(2), 2a(2)) \circledast (2b(0) + 24b(1), 2b(1) + 6b(2), 2b(2)) = (26a(0) + 3a(1) + 2b(0) + 24b(1) + 18a(0)a(2)b(1) + 9a(0)b(1)b(2) + 9a(1)a(2)b(0) + 18a(1)b(0)b(2), 8a(1) + 3a(2) + 2b(1) + 6b(2), 2a(2) + 2b(2))$ and $a \bigtriangledown_2 b = \mathbf{x} \cdot a \boxtimes (1 - \mathbf{x}) \cdot b = (26a(0) + 3a(1), 8a(1) + 3a(2), 2a(2)) \boxtimes (2b(0) + 24b(1), 2b(1) + 6b(2), 2b(2)) = (26a(0) + 3a(1) + 2b(0) + 24b(1) + 9a(0)a(2)b(1) + 18a(0)b(1)b(2) + 18a(1)a(2)b(0) + 9a(1)b(0)b(2), 8a(1) + 3a(2) + 2b(1) + 6b(2), 2a(2) + 2b(2))$ for all $a, b \in \mathcal{C}$; we have $a \bigtriangledown_2 b = (a \bigtriangledown_1 b) - \tau_1(a, b, a - b) = (a \bigtriangledown_1) + \tau_2(a, b, a - b)$ and $\mathcal{C}(\bigtriangledown_1) = \mathcal{D}_2(\bigtriangledown)$ (see 3.2). The permutation ξ of $\mathcal{C}$ is an anti–isomorphism of $\mathcal{C}(\bigtriangledown_1)$ onto $\mathcal{C}(\bigtriangledown_2)$, i.e. $\xi(a \bigtriangledown_1 b) = \xi(b) \bigtriangledown_2 \xi(a)$ for all $a, b \in \mathcal{C}$ (see 12.2.3 and 12.4.3).

12.8 Theorem. (i) *Every non–medial hamiltonian distributive quasigroup has at least 729 elements.*
(ii) *$\mathcal{C}(\bigtriangledown_1)$ and $\mathcal{C}(\bigtriangledown_2)$ are (up to isomorphism) the only non–medial hamiltonian distributive quasigroups of order 729; these two quasigroups are not isomorphic, but they are anti–isomorphic.*

Proof. Combine 7.7, 9.1, 9.2, 9.3, 12.6 and 12.7. $\square$

12.9 Remark. The preceding theorem says that up to usual equivalences (as isomorphism and parastrophy) there exists only one non-medial hamiltonian distributive quasigroup of order 729, which is the smallest possible order for such

a structure. The mapping $a \mapsto (18a(0)^3 + 9a(0)^2a(1) + 18a(0)a(1)^2 + 10a(0), a(0) + 8a(1), a(0)+a(1)+a(2))$ is an anti–isomorphism of $\mathcal{C}(\bigtriangledown_1)$ onto $\mathcal{C}(\bigtriangledown_2)$, and so $\mathcal{C}(\bigtriangledown_2)$ is isomorphic to the opposite quasigroup $\overline{\mathcal{C}(\bigtriangledown_1)}$.

12.10 Remark. Using 12.4.5 (and also 12.4.4 and 12.9), we come to the following isomorphisms for the parastrophes of the quasigroups $\mathcal{C}(\bigtriangledown_1)$ and $\mathcal{C}(\bigtriangledown_2)$: $\mathcal{C}(\bigtriangledown_2) \simeq \overline{\mathcal{C}(\bigtriangledown_1)} \simeq \mathcal{C}(\bigtriangledown_1)^{-1} \simeq {}^{-1}\mathcal{C}(\bigtriangledown_1)$, $\mathcal{C}(\bigtriangledown_1) \simeq \overline{\mathcal{C}(\bigtriangledown_2)} \simeq \mathcal{C}(\bigtriangledown_2)^{-1} \simeq {}^{-1}\mathcal{C}(\bigtriangledown_2)$.

References

1. F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Graduate Texts in Mathematics 13, Springer Verlag, 1992.
2. V. D. Belousov, *Dve zadači po distributivnym kvazigruppam*, Issled. po algebre i mat. analizu, Kishinev, 1965, pp. 109–112.
3. ———, *Osnovy teorii kvazigrupp i lup*, Nauka, Moskva, 1967.
4. L. Bénéteau, *Free commutative Moufang loops and anticommutative graded rings*, J. Algebra **67** (1980), 1–35.
5. L. Bénéteau and T. Kepka, *Théorèmes de structure dans certains groupoïdes localement nilpotent*, C. R. Acad. Sci. Paris, t. 300, Série I, n^o 11 (1985), 327–330.
6. ———, *Quasigroupes trimédiaux et boucles de Moufang commutatives libres*, C. R. Acad. Sci. Paris, t. 300, Série I, n^o 12 (1985), 377–380.
7. L. Bénéteau, T. Kepka and J. Lacaze, *Small finite trimedial quasigroups*, Commun. Algebra **14** (1986), 1067–1090.
8. L. Bican, T. Kepka and P. Němec, *Rings, Modules, and Preradicals*, Lecture Notes in Pure and Appl. Math. 75, Marcel Dekker, Inc., New York and Basel, 1982.
9. G. Bol, *Gewebe und Gruppen*, Math. Ann. **114** (1937), 414–431.
10. R. H. Bruck, *A Survey of Binary Systems*, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.
11. C. Burstin and W. Mayer, *Distributive Gruppen von endlicher Ordnung*, J. Reine Angew. Math. **160** (1929), 111–130.
12. O. Chein, H. O. Pflugfelder and J. D. H. Smith (Eds.), *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.
13. R. Dedekind, *Über Gruppen, deren sämtliche Teiler Normalteiler sind*, Math. Ann. **48** (1897), 548–561.
14. A. Facchini, *Module Theory. Endomorphism rings and direct sum decompositions in some classes of modules*, Progress in Math. 167, Birkhäuser Verlag, Basel, 1998.
15. B. Fischer, *Distributive Quasigruppen endlicher Ordnung*, Math. Z. **83** (1964), 267–303.
16. R. Fossum, *The structure of indecomposable injective modules*, Math. Scand. **36** (1975), 291–312.
17. M. Hall, Jr., *Automorphisms of Steiner triple systems*, IBM J. Res. Develop. (1960), 460–472.
18. J. Ježek and T. Kepka, *Varieties of abelian quasigroups*, Czech. Math. J. **27** (1977), 473–503.
19. T. Kepka, *Structure of triabelian quasigroups*, Comment. Math. Univ. Carolinae **17** (1976), 229–240.
20. ———, *Distributive Steiner quasigroups of order* 3^5, Comment. Math. Univ. Carolinae **19** (1978), 389–401.
21. ———, *Notes on quasimodules*, Comment. Math. Univ. Carolinae **20** (1979), 229–24.
22. ———, *Hamiltonian quasimodules and trimedial quasigroups*, Acta Univ. Carolinae Math. Phys. **26** (1985), no. 1, 11–20.
23. T. Kepka and P. Němec, *T-quasigroups I*, Acta Univ. Carolinae Math. Phys. **12,1** (1971), 39–49.
24. ———, *T-quasigroups II*, Acta Univ. Carolinae Math. Phys. **12,2** (1971), 31–49.
25. ———, *Quasimodules generated by three elements*, Comment. Math. Univ. Carolinae **20** (1979), 249–266.
26. ———, *Trilinear constructions of quasimodules*, Comment. Math. Univ. Carolinae **21** (1980), 341–354.
27. ———, *Commutative Moufang loops and distributive groupoids of small orders*, Czech. Math. J. **31** (1981), 633–669.
28. ———, *Torsion quasimodules*, Comment. Math. Univ. Carolinae **25** (1984), 699–717.

29. ———, *Trimedial quasigroups and generalized modules I*, Acta Univ. Carolinae Math. Phys. **31** (1990), no. 1, 3–14.
30. A. S. McKerrow, *On the injective dimensions of modules of power series*, Quart. J. Math. Oxford **25** (1974), 359–368.
31. S. Klossek, *Kommutative Spiegelungräume*, Mitt. Math. Sem. Giessen Heft 117, Giessen, 1975.
32. A. N. Kolmogorov, *Sur la notion de moyenne*, Atti della R. Acad. Nazion. dei Lincei **12** (1930).
33. F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge tracts 19, Cambridge University Press, Cambridge, 1916.
34. J. P. Malbos, *Sur la classe de nilpotence des BMC et des espaces médiaux*, C. R. Acad. Sci. Pairs, Série A **287** (1978), 691–693.
35. Ju. I. Manin, *Kubičeskie formy*, Nauka, Moskva, 1972.
36. H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1990.
37. D. G. Northcott, *Injective envelopes and inverse polynomials*, J. London Math. Soc. **(2)8** (1974), 290–296.
38. D. A. Norton, *Hamiltonian loops*, Proc. Amer. Math. Soc. **3** (1952), 56–65.
39. C. S. Peirce, *On the algebra of logic*, Amer. J. Math. **III** (1880), 15–57.
40. H. O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann, Berlin, 1990.
41. N. I. Sandu, *O stroenii CH–kvazigrupp*, Izv. AN MSSR (1980), 9–15.
42. N. I. Sandu and V. I. Onoj, *O distributivnych kvazigruppach i CH–kvazigruppach*, Issled. po sovremennoj algebre i geometrii, Štiinca, Kišinev, 1983, pp. 116–123.
43. E. Schröder, *Über Algorithmen und Calculi*, Arch. der Math. und Phys., 2^{nd} series **5** (1887), 225–278.
44. D. W. Sharpe and P. Vamos, *Injective Modules*, Cambridge tracts in Math. and Math. Physics, Cambridge University Press, Cambridge, 1972.
45. J. D. H. Smith, *On the nilpotence class of commutative Moufang loops*, Math. Proc. Cambridge Phil. Soc. **84** (1978), 387–404.
46. J. P. Soublin, *Médiations*, C. R. Acad. Sci. Paris, Série A–B **263** (1966), A49–A50.
47. ———, *Médiations*, C. R. Acad. Sci. Paris, Série A–B **263** (1966), A115–A117.
48. ———, *Etude algébrique de la notion de moyenne*, J. Math. Pures Appl. **50** (1971), 53–264.
49. A. K. Suškevič, *Teorija obobščennych grupp*, Gos. Nauč.–Tech. Izd. Ukrainy, Charkov–Kiev, 1936.
50. N. Wisbauer, *Grundlagen der Modul- und Ringtheorie*, Verlag R. Fischer, München, 1988.

Department de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
E-mail address: dolors@mat.uab.es

Department of Algebra, MFF UK, Sokolovská 83, 186 75 Praha 8, Czech Republic
E-mail address: kepka@karlin.mff.cuni.cz

Department of Mathematics, ČZU, Kamýcká 129, 165 21 Praha 6 – Suchdol, Czech Republic
E-mail address: nemec@tf.czu.cz